Autenticación de vSphere

Actualización 3

VMware vSphere 8.0
VMware ESXi 8.0
vCenter Server 8.0

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware by Broadcom en:

https://docs.vmware.com/es/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contenido

Acerca de *vSphere Authentication*

La documentación de *vSphere Authentication* proporciona información para ayudarle a realizar tareas comunes, como la administración de certificados y la configuración de vCenter Single Sign-On.

En VMware, valoramos la inclusión. Para fomentar este principio dentro de nuestra comunidad de clientes, socios y personal interno, creamos contenido con un lenguaje inclusivo.

vSphere Authentication explica cómo administrar certificados para vCenter Server y servicios relacionados, y cómo configurar la autenticación con vCenter Single Sign-On.

Tabla 1-1. Información destacada de *vSphere Authentication*

Temas	Contenido destacado
Introducción a la autenticación	■ Administración de servicios de autenticación. ■ Administración de vCenter Server mediante la interfaz de administración de vCenter Server.
Certificados de seguridad de vSphere	■ Modelo de certificado y opciones de reemplazo de certificados. ■ Reemplazo de certificados desde la interfaz de usuario (casos simples). ■ Reemplazo de certificados mediante la utilidad Certificate Manager. ■ Reemplazo de certificados mediante la CLI (situaciones complejas). ■ Referencia de la CLI para la administración de certificados.
Autenticar vSphere con vCenter Single Sign-On	■ Arquitectura del proceso de autenticación. ■ Forma de agregar orígenes de identidad para que los usuarios del dominio se puedan autenticar. ■ Autenticación de dos factores. ■ Administración de usuarios, grupos y directivas. ■ vCenter Server Federación de proveedor de identidad

Qué ocurrido con Platform Services Controller

A partir de vSphere 7.0, la implementación de una nueva instancia de vCenter Server o la actualización a vCenter Server 7.0 requiere el uso de vCenter Server Appliance, una máquina virtual preconfigurada y optimizada para ejecutar vCenter Server. La nueva instancia de vCenter Server contiene todos los servicios de Platform Services Controller y conserva la funcionalidad

y los flujos de trabajo, incluidos la autenticación, la administración de certificados, las etiquetas y la concesión de licencias. Ya no es necesario ni es posible implementar y utilizar una instancia de Platform Services Controller externa. Todos los servicios de Platform Services Controller se consolidan en vCenter Server, y se simplifican la implementación y la administración.

Dado que estos servicios ahora forman parte de vCenter Server, ya no se describen como parte de Platform Services Controller. En vSphere 7.0, la publicación de *vSphere Authentication* reemplaza la publicación de *Administrar Platform Services Controller*. La nueva publicación contiene información completa sobre la autenticación y la administración de certificados. Para obtener información sobre la actualización o la migración de las implementaciones de vSphere 6.5 y 6.7 con una instancia externa existente de Platform Services Controller a vSphere 7.0 mediante vCenter Server Appliance, consulte la documentación de *Actualizar vSphere*.

Documentación relacionada

En un documento complementario, *Seguridad de vSphere*, se describen las medidas y las características de seguridad disponibles que se pueden llevar a cabo para proteger el entorno frente a ataques. En ese documento también se explica cómo se configuran los permisos y se incluye una referencia a los privilegios.

Además de estos documentos, VMware publica la *guía de configuración de seguridad de vSphere* (anteriormente denominada la *Guía de fortalecimiento*) para cada versión de vSphere. Puede obtener dicha guía en https://core.vmware.com/security. La *guía de configuración de seguridad de vSphere* contiene directrices de configuración de seguridad que el cliente puede o debe definir, así como la configuración de seguridad proporcionada por VMware que el cliente debe auditar para garantizar que aún tiene el valor predeterminado.

Audiencia prevista

Esta información está dirigida a administradores que desean configurar la autenticación de vCenter Server y sus servicios asociados, así como administrar certificados. La información está destinada a administradores de sistemas Linux con experiencia y que están familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Introducción a la autenticación y la administración de certificados de vSphere

1

vSphere proporciona servicios de infraestructura comunes para administrar certificados para componentes de vCenter Server y ESXi, así como para administrar la autenticación con vCenter Single Sign-On.

Cómo administrar certificados de vSphere

De forma predeterminada, vSphere permite aprovisionar componentes de vCenter Server y hosts ESXi con certificados de VMware Certificate Authority (VMCA). También puede utilizar certificados personalizados que se almacenan en VMware Endpoint Certificate Store (VECS). Para obtener más información, consulte Qué opciones tiene para administrar certificados de vSphere.

Qué es vCenter Single Sign-On

vCenter Single Sign-On permite que los componentes de vSphere se comuniquen entre sí a través de un mecanismo de token seguro. vCenter Single Sign-On utiliza términos y definiciones específicos que resulta importante comprender.

Tabla 1-1. Glosario de vCenter Single Sign-On

Término	Definición
Principal	Una entidad que se puede autenticar, como un usuario.
Proveedor de identidad	Un servicio que administra orígenes de identidad y autentica entidades de seguridad. Ejemplos: Servicios de federación de Active Directory (Active Directory Federation Services, AD FS) de Microsoft y vCenter Single Sign-On.
Origen de identidad (servicio de directorio)	Almacena y administra entidades de seguridad. Las entidades de seguridad consisten en una colección de atributos sobre una cuenta de usuario o un servicio, como el nombre, la dirección, el correo electrónico y la membresía a grupos. Ejemplos: Microsoft Active Directory y VMware Directory Service (vmdir).

Tabla 1-1. Glosario de vCenter Single Sign-On (continuación)

Término	Definición
Autenticación	Los medios para determinar si alguien o algo es efectivamente quién o qué declara ser. Por ejemplo, los usuarios se autentican cuando proporcionan sus credenciales, como tarjetas inteligentes, nombre de usuario y contraseña correctos, etc.
Autorización	El proceso de comprobación de los objetos a los que las entidades de seguridad tienen acceso.
Token	Una recopilación firmada de datos que incluye la información de identidad de una entidad de seguridad determinada. Un token puede incluir no solo información básica sobre la entidad de seguridad, como la dirección de correo electrónico y el nombre completo, sino también, según el tipo de token, los grupos y las funciones de la entidad de seguridad.
vmdir	VMware Directory Service. El repositorio LDAP interno (local) en vCenter Server que contiene identidades de los usuarios, grupos y datos de configuración.
OAuth 2.0	Un estándar de autorización abierta que permite el intercambio de información entre entidades de seguridad y servicios web sin exponer las credenciales de las entidades de seguridad.
OpenID Connect (OIDC)	Protocolo de autenticación basado en OAuth 2.0 que aumenta OAuth con información de identificación del usuario. Se representa mediante el token de identificador que el servidor de autorización devuelve junto con el token de acceso durante la autenticación de OAuth. vCenter Server utiliza capacidades de OIDC al interactuar con los servicios de federación de Active Directory (Active Directory Federation Services, AD FS), Okta, Microsoft Entra ID y PingFederate.
Sistema para la administración de identidades entre dominios (SCIM)	El estándar para automatizar el intercambio de información de la identidad del usuario entre dominios de identidad o sistemas de TI.
VMware Identity Services	A partir de la versión 8.0 Update 1, VMware Identity Services es un contenedor integrado dentro de vCenter Server que se puede utilizar para la federación de identidades en proveedores de identidad externos. Funciona como un agente de identidad independiente dentro de vCenter Server y viene con su propio conjunto de API. Actualmente, VMware Identity Services admite Okta, Microsoft Entra ID y PingFederate como proveedores de identidad externos.
Tenant	Un concepto de VMware Identity Services. Un tenant proporciona una separación lógica de los datos de otros tenants en un mismo entorno virtual.

Tabla 1-1. Glosario de vCenter Single Sign-On (continuación)

Término	Definición
Token de Web JSON (JWT)	Formato de token definido por la especificación de OAuth 2.0. Un token JWT transmite información de autenticación y autorización sobre una entidad de seguridad.
Usuario de confianza	Un usuario de confianza "depende" del servidor de autorización, VMware Identity Services o AD FS para la administración de identidades. Por ejemplo, a través de la federación, vCenter Server establece una relación de confianza entre el usuario dependiente con VMware Identity Services o AD FS.
Lenguaje de marcado de aserción de seguridad (SAML)	Un estándar abierto basado en XML para intercambiar datos de autenticación y autorización entre partes que utiliza vCenter Server. Las entidades de seguridad obtienen un token SAML de parte de vCenter Single Sign-On y, a continuación, lo envían al endpoint de la API de vSphere Automation para obtener un identificador de sesión.

Descripción de los tipos de autenticación de vCenter Single Sign-On

vCenter Single Sign-On utiliza diferentes tipos de autenticación, en función de si está implicado el proveedor de identidad vCenter Server integrado o un proveedor de identidad externo.

Tabla 1-2. Tipos de autenticación de vCenter Single Sign-On

Tipo de autenticación	¿Qué actúa como el proveedor de identidad?	¿vCenter Server gestiona la contraseña?	Descripción
Autenticación basada en token	Proveedor de identidad externo. Por ejemplo, AD FS.	No	vCenter Server se comunica con el proveedor de identidad externo a través de un protocolo en particular y obtiene un token, que representa una identidad de usuario en particular.
Autenticación simple	vCenter Server	Sí	El nombre de usuario y la contraseña se transmiten directamente a vCenter Server, que valida las credenciales a través de sus orígenes de identidad.

Lea los siguientes temas a continuación:

- Administración de certificados de vCenter Server
- Administrar servicios de autenticación de vCenter Server

- Administrar vCenter Server

Administración de certificados de vCenter Server

Los certificados de vCenter Server se administran desde vSphere Client o mediante una API, scripts y CLI.

En la siguiente tabla se describen las interfaces que puede utilizar para administrar certificados de vCenter Server.

Tabla 1-3. Interfaces para administrar certificados de vSphere

Interfaz	Descripción
vSphere Client	Interfaz web (cliente basado en HTML5). Consulte Administrar certificados mediante el vSphere Client.
vSphere Automation API	Consulte *Guía de programación de VMware vSphere Automation SDK*.
Utilidad de administración de certificados	Herramienta de línea de comandos que admite la generación de la solicitud de firma del certificado (Certificate Signing Request, CSR) y el reemplazo certificados. Consulte Administrar certificados mediante la utilidad de vSphere Certificate Manager.
CLI para administrar servicios de certificados y directorios	Conjunto de comandos para administrar certificados, VMware Endpoint Certificate Store (VECS) y VMware Directory Service (vmdir). Consulte Capítulo 3 Referencia de comandos de CLI de servicios y certificados de vSphere.

Administrar certificados de vCenter Server mediante vSphere Client

Puede administrar certificados de vCenter Server desde vSphere Client.

Procedimiento

1 Inicie sesión en vCenter Server como usuario con privilegios de administrador en el dominio local de vCenter Single Sign-On.

   El dominio predeterminado es vsphere.local.

2 Seleccione **Administración**.

3 En **Certificados**, haga clic en **Administración de certificados**.

   Aparecen pestañas de certificados para los distintos tipos de certificados.

4 Realice tareas de certificado, como ver los detalles del certificado, renovar o actualizar un certificado, y agregar un certificado raíz de confianza.

   Para obtener más información, consulte Administrar certificados mediante el vSphere Client.

Administrar certificados vCenter Server mediante CLI

vCenter Server incluye CLI para generar solicitudes de firma del certificado (Certified Signing Requests, CSR), administrar certificados y administrar servicios.

Por ejemplo, puede usar el comando `certool` para generar CSR y para reemplazar los certificados.

Use las CLI para tareas de administración que vSphere Client no admita o para crear scripts personalizados para el entorno.

Tabla 1-4. CLI para administrar certificados y servicios relacionados de vCenter Server

CLI	Descripción	Vínculos
`certool`	Genere y administre certificados y claves. Parte de VMware Certificate Authority (VMCA).	Referencia de comandos de inicialización de certool
`vecs-cli`	Administre el contenido de las instancias de VMware Certificate Store. Parte de VMware Authentication Framework Daemon (VMAFD).	Referencia de comandos vecs-cli
`dir-cli`	Cree y actualice los certificados en VMware Directory Service. Parte de VMAFD.	Referencia de comando dir-cli
`sso-config`	Actualice los certificados del servicio de token de seguridad (STS).	Reemplazar un certificado vCenter Server STS mediante la línea de comandos
`service-control`	Comando para iniciar, detener y armar una lista de servicios.	Ejecute este comando para detener los servicios antes de ejecutar otros comandos de la CLI.

Requisitos previos

Habilitar inicio de sesión en SSH en vCenter Server. Puede utilizar la pestaña **Acceso** de la interfaz de administración de vCenter Server (`https://`*`vcenter_server_ip`*`:5480`) para activar y desactivar el inicio de sesión SSH.

Procedimiento

1 Inicie sesión en el shell de vCenter Server.

Generalmente, debe ser el usuario raíz o administrador. Consulte Privilegios necesarios para ejecutar las CLI de vSphere para obtener detalles.

2 Acceda a la CLI en una de las siguientes ubicaciones predeterminadas.

Los privilegios necesarios dependen de la tarea que se desea realizar. En algunos casos, se solicita que introduzca la contraseña dos veces para proteger información confidencial.

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

El comando `service-control` no requiere que introduzca la ruta de acceso.

Para obtener más información, consulte Reemplazar certificados de vSphere de forma manual.

Administrar servicios de autenticación de vCenter Server

Los servicios de autenticación se administran desde la instancia de vSphere Client o mediante la CLI. También puede administrar el proceso de configuración de la federación de proveedores de identidad de vCenter Server mediante una API.

Puede administrar la autenticación de vCenter Server con diferentes interfaces.

Tabla 1-5. Interfaces para administrar servicios de autenticación de vCenter Server

Interfaz	Descripción
vSphere Client	Interfaz web (cliente basado en HTML5).
API	Administre el proceso de configuración de la federación de proveedores de identidad de vCenter Server.
`sso-config`	Utilidad de línea de comandos para configurar el proveedor de identidad integrado de vCenter Server.

Administrar vCenter ServerServicios de autenticación mediante vSphere Client

Puede administrar servicios de autenticación de vCenter Server desde la instancia de vSphere Client.

Procedimiento

1 Inicie sesión en vCenter Server como usuario con privilegios de administrador en el dominio local de vCenter Single Sign-On.

El dominio predeterminado es vsphere.local.

2 Seleccione **Administración**.

3 En **Single Sign-On**, haga clic en **Configuración** para administrar los proveedores de identidad y configurar las directivas de contraseñas y bloqueo.

Para obtener más información, consulte Capítulo 4 Autenticar vSphere con vCenter Single Sign-On.

Administrar vCenter Server servicios de autenticación mediante scripts

vCenter Server incluye una utilidad, `sso-config`, para administrar servicios de autenticación.

Use la utilidad `sso-config` para tareas de administración que vSphere Client no admite o para crear scripts personalizados para el entorno.

Tabla 1-6. CLI para administrar servicios de autenticación y relacionados

CLI	Descripción	Vínculos
`sso-config`	Utilidad de línea de comandos para configurar el proveedor de identidad integrado de vCenter Server.	Para consultar la ayuda de `sso-config`, ejecute `sso-config.sh -help` o vea el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/67304 para obtener ejemplos de uso.
`service-control`	Comando para iniciar, detener y armar una lista de servicios.	Ejecute este comando para detener los servicios antes de ejecutar otros comandos de la CLI. El comando `service-control` no requiere que especifique la ruta de acceso.

Requisitos previos

Habilitar inicio de sesión en SSH en vCenter Server. Puede utilizar la pestaña **Configuración de acceso** de la interfaz de administración de vCenter Server (`https://`*`vcenter_server_ip`*`:5480`) para activar y desactivar el inicio de sesión SSH.

Procedimiento

1 Inicie sesión en el shell de vCenter Server.

Generalmente, debe ser el usuario raíz o administrador. Consulte Privilegios necesarios para ejecutar las CLI de vSphere para obtener detalles.

2 Acceda a la utilidad `sso-config` en la siguiente ubicación predeterminada.

```
/opt/vmware/bin/sso-config.sh
```

Los privilegios necesarios dependen de la tarea que se desea realizar. En algunos casos, se solicita que introduzca la contraseña dos veces para proteger información confidencial.

Administrar vCenter Server

vCenter Server se puede administrar desde la interfaz de administración de vCenter Server o desde el shell de vCenter Server.

Para obtener más información sobre cómo administrar vCenter Server, consulte *Configuración de vCenter Server*.

Tabla 1-7. Interfaces para administrar vCenter Server

Interfaz	Descripción
Interfaz de administración de vCenter Server	Utilice esta interfaz para volver a configurar las opciones del sistema. Consulte Administrar vCenter Server mediante la interfaz de administración.
Shell de vCenter Server	Use esta interfaz de línea de comandos para realizar operaciones de administración de servicios en VMCA, VECS y VMDIR. Consulte Administrar certificados mediante la utilidad de vSphere Certificate Manager y Capítulo 3 Referencia de comandos de CLI de servicios y certificados de vSphere.

Administrar vCenter Server mediante la interfaz de administración

Puede usar la interfaz de administración de vCenter Server para configurar las opciones del sistema.

La configuración de la interfaz de administración de vCenter Server incluye sincronización de hora, configuración de red y configuración de inicio de sesión SSH. También es posible cambiar la contraseña raíz, unir el dispositivo a un dominio de Active Directory y abandonar un dominio de Active Directory.

Nota En el panel **Redes**, la NIC virtual 0 está reservada para el tráfico de administración. No se puede reasignar el tráfico de la NIC 0 a otra NIC. Si utiliza VCHA, este tráfico utiliza la NIC 1. Puede agregar NIC al vCenter Server Appliance. Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/article/2147155.

Procedimiento

1 En un explorador, vaya a la interfaz web en `https://`*`vcenter_server_ip`*`:5480`.

2 Si aparece un mensaje de advertencia sobre un certificado SSL que no es de confianza, solucione el problema en función de la directiva de seguridad de la empresa y el explorador que está usando.

3 Inicie sesión como raíz.

  La contraseña raíz predeterminada es la contraseña raíz que estableció al implementar vCenter Server.

Resultados

Verá la página Resumen de la interfaz de administración de vCenter Server.

Administrar vCenter Server mediante el shell de vCenter Server

Puede emplear utilidades de administración de servicios y CLI desde el shell de vCenter Server. Puede usar TTY1 para iniciar sesión en la consola, o bien SSH para conectarse al shell.

Procedimiento

1 Active el inicio de sesión SSH si es necesario.

   a Inicie sesión en la interfaz de administración de vCenter Server en https://*vcenter_server_ip*:5480.

   b En el navegador, seleccione **Acceso** y haga clic en **Editar**.

   c Active **Activar el inicio de sesión SSH** y haga clic en **Aceptar**.

   Puede seguir los mismos pasos para activar el shell de Bash para vCenter Server.

2 Acceda al shell.

   - Si tiene acceso directo a la consola de vCenter Server, seleccione **Iniciar sesión** y presione Intro.
   - Para conectarse de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en vCenter Server.

3 Inicie sesión como raíz con la contraseña que configuró mientras implementaba inicialmente vCenter Server.

   Si cambió la contraseña raíz, use la nueva contraseña.

Agregar una instancia de vCenter Server a un dominio de Active Directory

Si desea agregar un origen de identidad de Active Directory a vCenter Server, primero debe unir la instancia de vCenter Server a un dominio de Active Directory.

Si no puede utilizar la federación de proveedores de identidad de vCenter Server o Active Directory en LDAP, vCenter Server admite la autenticación integrada de Windows (Integrated Windows Authentication, IWA). Para usar IWA, debe unir vCenter Server con el dominio de Active Directory.

Procedimiento

1 Mediante vSphere Client, inicie sesión en vCenter Server como usuario con privilegios de administrador en el dominio de vCenter Single Sign-On local (vsphere.local de manera predeterminada).

2 Seleccione **Administración**.

3 Expanda **Single Sign-On** y haga clic en **Configuración**.

4 En la pestaña **Proveedor de identidad**, haga clic en **Dominio de Active Directory**.

5 Haga clic en **Unirse a AD**, especifique el dominio, la unidad organizativa opcional, un nombre de usuario y una contraseña; a continuación, haga clic en **Unirse**.

6 Reinicie vCenter Server.

Pasos siguientes

Para asociar usuarios y grupos del dominio de Active Directory al que se unió, agregue dicho dominio como un origen de identidad de vCenter Single Sign-On. Consulte Agregar o editar un origen de identidad vCenter Single Sign-On.

Certificados de seguridad de vSphere

2

vSphere proporciona seguridad mediante el uso de certificados para cifrar las comunicaciones, autenticar los servicios y firmar tokens.

Cómo utilizar certificados de vSphere

vSphere utiliza certificados para:

- Cifrar las comunicaciones entre dos nodos, por ejemplo, vCenter Server y un host ESXi.
- Autenticar los servicios de vSphere.
- Realizar acciones internas, como firmar tokens.

Qué es VMware Certificate Authority

La entidad de certificación interna de vSphere, VMware Certificate Authority (VMCA) proporciona todos los certificados necesarios para vCenter Server y ESXi. VMCA se instala en cada host vCenter Server de manera que la solución queda protegida de forma inmediata sin tener que modificar nada más. Mantener esta configuración predeterminada proporciona la sobrecarga operativa más baja para la administración de certificados. vSphere proporciona un mecanismo para renovar estos certificados en caso de que caduquen.

vSphere también proporciona un mecanismo para reemplazar determinados certificados con sus propios certificados. Sin embargo, reemplace solamente el certificado SSL que proporciona cifrado entre los nodos, para reducir la sobrecarga de administración de certificados al mínimo.

Qué opciones tiene para administrar certificados de vSphere

Se recomiendan las siguientes opciones para la administración de certificados.

Tabla 2-1. Opciones recomendadas para administrar certificados de vSphere

Modo	Descripción	Ventajas
Certificados de VMCA predeterminados	VMCA proporciona todos los certificados para hosts de vCenter Server y de ESXi.	Sobrecarga más simple y más baja. VMCA puede administrar el ciclo de vida de certificados para vCenter Server y hosts ESXi.
Certificados de VMCA predeterminados con certificados SSL externos (modo híbrido)	Para administrar certificados de los usuarios de solución y los hosts ESXi, debe reemplazar los certificados SSL de vCenter Servery permitir VMCA. De manera opcional, para las implementaciones de alta seguridad conscientes, puede reemplazar también los certificados SSL de host ESXi.	Simple y seguro. VMCA administra los certificados internos, pero se obtiene el beneficio de obtener sus certificados SSL aprobados por la empresa y que los exploradores confíen en dichos certificados.

Qué herramientas están disponibles para reemplazar certificados de vSphere

Puede utilizar las siguientes opciones para reemplazar los certificados existentes.

Tabla 2-2. Diferentes enfoques de reemplazo de certificados de vSphere

Opción	Consulte
Utilice vSphere Client.	Administrar certificados mediante el vSphere Client
Utilice vSphere Automation API para administrar el ciclo de vida de los certificados.	*Guía de programación de VMware vSphere Automation SDK*
Ejecute la utilidad vSphere Certificate Manager desde la línea de comandos.	Administrar certificados mediante la utilidad de vSphere Certificate Manager
Utilice los comandos de la CLI para el reemplazo manual de certificados.	Capítulo 3 Referencia de comandos de CLI de servicios y certificados de vSphere

Lea los siguientes temas a continuación:

- Requisitos de certificados de vSphere para distintas rutas de acceso de la solución
- Administración de certificados de vSphere
- Administrar certificados mediante el vSphere Client
- Administrar certificados mediante la utilidad de vSphere Certificate Manager
- Reemplazar certificados de vSphere de forma manual

Requisitos de certificados de vSphere para distintas rutas de acceso de la solución

Los requisitos de certificados dependen de si se usa VMware Certificate Authority (VMCA) como entidad de certificación intermedia o si se usan certificados personalizados. Los requisitos también son diferentes para los certificados de máquina.

Antes de comenzar a modificar certificados, asegúrese de que la hora de todos los nodos del entorno de vSphere esté sincronizada.

Nota vSphere implementa solo certificados RSA para la autenticación del servidor y no permite que se generen certificados ECDSA. vSphere verifica los certificados ECDSA que presenten otros servidores. Por ejemplo, si vSphere se conecta a un servidor syslog y el servidor syslog tiene un certificado ECDSA, vSphere permitirá que se verifique ese certificado.

Requisitos para todos los certificados de vSphere importados

- Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM). vSphere Client y la API siguen aceptando un tamaño de clave de hasta 16.384 bits al generar la solicitud de firma del certificado.

  Nota En vSphere 8.0, solo se pueden generar CSR con una longitud de clave mínima de 3072 bits cuando se utiliza vSphere Client o vSphere Certificate Manager. vCenter Server aún acepta certificados personalizados con una longitud de clave de 2048 bits. En vSphere 8.0 Update 1 y versiones posteriores, puede utilizar vSphere Client para generar una CSR con una longitud de clave de 2048 bits.

  Nota El certificado FIPS de vSphere solo valida los tamaños de clave RSA de 2048 y 3072 bits.

- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
- x509 versión 3
- SubjectAltName debe contener DNS Name=*machine_FQDN*
- Formato CRT
- Contiene los siguientes usos de claves: firma digital, cifrado de clave.
- Si se excluye el certificado de usuario de la solución vpxd-extension, Uso mejorado de clave puede estar vacío o contener autenticación de servidor.

vSphere no admite los siguientes certificados.

- Certificados con comodines.
- No se admiten los algoritmos md2WithRSAEncryption, md5WithRSAEncryption, RSASSA-PSS, dsaWithSHA1, ecdsa_with_SHA1 y sha1WithRSAEncryption.

- Al crear un certificado SSL de máquina personalizado para vCenter Server, la autenticación de servidor y la autenticación de cliente no son compatibles y deben eliminarse cuando se utilizan plantillas de entidad de certificación (CA) de Microsoft. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2112009.

Cumplimiento del certificado de vSphere con RFC 2253

El certificado debe cumplir con RFC 2253.

Si no genera solicitudes de firma de certificados (Certificate Signature Request, CSR) con vSphere Certificate Manager, asegúrese de que la CSR incluya los siguientes campos.

Cadena	Tipo de atributo X.500
CN	`commonName`
L	`localityName`
ST	`stateOrProvinceName`
O	`organizationName`
OU	`organizationalUnitName`
C	`countryName`
CALLE	`streetAddress`
DC	`domainComponent`
UID	`userid`

Si genera las CSR mediante vSphere Certificate Manager, se le pedirá la siguiente información y vSphere Certificate Manager agregará los campos correspondientes al archivo de CSR.

- La contraseña del usuario administrator@vsphere.local o del administrador del dominio de vCenter Single Sign-On al que se va a conectar.
- Información que vSphere Certificate Manager almacena en el archivo `certool.cfg`. En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.
  - Contraseña de administrator@vsphere.local
  - Código de país de dos letras
  - Nombre de empresa
  - Nombre de organización
  - Unidad de organización
  - Estado
  - Localidad
  - Dirección IP (opcional)
  - Correo electrónico

- Nombre del host, es decir, el nombre de dominio completo de la máquina para la que se desea reemplazar el certificado. Si el nombre del host no coincide con el FQDN, el reemplazo de los certificados no se completa correctamente y el entorno puede quedar en un estado inestable.
- Dirección IP del nodo de vCenter Server en el que se ejecuta vSphere Certificate Manager.

Nota El campo OU (organizationalUnitName) ya no es obligatorio.

Requisitos de certificación cuando se utiliza VMCA como entidad de certificación intermedia

Cuando se utiliza VMCA como entidad de certificación intermedia, los certificados deben cumplir los siguientes requisitos.

<table>
<tr><th>Tipo de certificado</th><th>Requisitos de certificados</th></tr>
<tr><td>Certificado raíz</td><td>

Se puede utilizar vSphere Certificate Manager para crear la CSR. Consulte Generar una CSR con Certificate Manager y preparar certificados raíz (CA intermedia).
Si prefiere crear la CSR de forma manual, el certificado que envíe para firmar debe cumplir con los siguientes requisitos.

Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
x509 versión 3
Para certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos. Por ejemplo:
<pre>basicConstraints   =
critical,CA:true
keyUsage   =
critical,digitalSignature,keyCertSign</pre>
La firma CRL debe estar habilitada.
Uso mejorado de clave puede estar vacío o contener autenticación del servidor.
No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados.
No se admiten los certificados con comodines o con más de un nombre DNS.
No se pueden crear CA subsidiarias de VMCA.
Para obtener un ejemplo de uso de la entidad de certificación de Microsoft, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2112009, Crear una plantilla de entidad de certificación de Microsoft para creación de certificados SSL en vSphere 6.x.

</td></tr>
<tr><td>Certificado SSL de máquina</td><td>
Se puede utilizar vSphere Certificate Manager para crear la solicitud CSR o crear manualmente la CSR.
Si crea la CSR manualmente, debe cumplir con los requisitos enumerados anteriormente en la sección Requisitos para todos los certificados de vSphere importados. También tendrá que especificar el FQDN del host.
</td></tr>
<tr><td>Certificado de usuario de solución</td><td>Se puede utilizar vSphere Certificate Manager para crear la solicitud CSR o crear manualmente la CSR.</td></tr>
</table>

Tipo de certificado	Requisitos de certificados
	Nota Debe utilizar un valor diferente en el nombre para cada usuario de solución. Si genera el certificado manualmente, es posible que esto se muestre como **CN** en el **asunto**, según la herramienta que utilice. Si utiliza vSphere Certificate Manager, la herramienta le solicitará información del certificado para cada usuario de solución. vSphere Certificate Manager almacena la información en `certool.cfg`. Para el usuario de solución vpxd-extension, puede dejar el uso de clave extendida vacío o utilizar "Autenticación de cliente WWW de TLS".

Requisitos cuando se utilizan certificados personalizados

Si desea utilizar certificados personalizados, los certificados deben cumplir los siguientes requisitos.

<table>
<tr><th>Tipo de certificado</th><th>Requisitos de certificados</th></tr>
<tr><td>Certificado SSL de máquina</td><td>El certificado SSL de máquina en cada nodo debe tener un certificado independiente de la entidad de certificación empresarial o externa.

Puede generar la CSR mediante vSphere Client o vSphere Certificate Manager, o bien puede crearla de forma manual. La CSR debe cumplir con los requisitos enumerados anteriormente en la sección Requisitos para todos los certificados de vSphere importados.
En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.
</td></tr>
<tr><td>Certificado de usuario de solución</td><td>Cada usuario de solución en cada nodo debe tener un certificado independiente de la entidad de certificación empresarial o externa.

Puede generar la CSR mediante vSphere Certificate Manager o prepararla usted mismo. La CSR debe cumplir con los requisitos enumerados anteriormente en la sección Requisitos para todos los certificados de vSphere importados.
Si utiliza vSphere Certificate Manager, la utilidad le solicitará información del certificado para cada usuario de solución. vSphere Certificate Manager almacena la información en <code>certool.cfg</code>.
Nota Debe utilizar un valor diferente en el nombre para cada usuario de solución. Un certificado generado manualmente se puede mostrar como CN en el asunto, según la herramienta que utilice.

Cuando reemplace posteriormente los certificados de usuario de solución por certificados personalizados, proporcione la cadena de certificados de firma completa de la entidad de certificación externa.
Para el usuario de solución vpxd-extension, puede dejar el uso de clave extendida vacío o utilizar "Autenticación de cliente WWW de TLS". </td></tr>
</table>

Administración de certificados de vSphere

El trabajo que se requiere para configurar o actualizar la infraestructura de certificados de vSphere depende de los requisitos de su entorno. Debe tener en cuenta si se está realizando una instalación nueva o una actualización, y si se está considerando ESXi o vCenter Server.

Entornos que usan certificados de VMware Certificate Authority

VMware Certificate Authority (VMCA) puede gestionar toda la administración de certificados. VMCA aprovisiona a vCenter Server con componentes y hosts ESXi con certificados que usan VMCA como entidad de certificación raíz. Si está actualizando a vSphere 6.0 o posterior desde una versión anterior de vSphere, todos los certificados autofirmados se reemplazan con certificados firmados por VMCA.

Si actualmente no reemplaza certificados de VMware, el entorno comienza a usar certificados firmados por VMCA en lugar de certificados autofirmados.

Entornos que utilizan certificados personalizados

Si la directiva de la empresa requiere certificados firmados por una entidad de certificación de terceros o empresarial, o que precisen información de certificados personalizados, existen varias opciones para una instalación nueva.

- Que el certificado raíz de VMCA sea firmado por una CA independiente o una CA empresarial. Reemplazar el certificado raíz de VMCA con ese certificado firmado. En este escenario, el certificado de VMCA es un certificado intermedio. VMCA aprovisiona a los componentes de vCenter Server y a los hosts ESXi con certificados que incluyen la cadena completa de certificados.
- Si la directiva de la empresa no permite certificados intermedios en la cadena, los certificados se pueden reemplazar de manera explícita. Puede usar la utilidad vSphere Client, vSphere Certificate Manager o realizar el reemplazo manual de los certificados mediante la CLI de administración de certificados.

Cuando actualice un entorno que usa certificados personalizados, puede retener algunos.

- Los hosts ESXi mantienen sus certificados personalizados durante la actualización. Asegúrese de que el proceso de actualización de vCenter Server agregue todos los certificados raíz relevantes al almacén TRUSTED_ROOTS en el almacén VECS (VMware Certificate Endpoint Store) en vCenter Server.

  Después de la actualización a vSphere 6.0 o versiones posteriores, se puede establecer el modo de certificado en **Personalizado**. Si el modo de certificado es VMCA, el predeterminado, y actualiza el certificado desde vSphere Client, los certificados firmados por VMCA reemplazarán a los certificados personalizados.
- En una actualización de una instalación simple de vCenter Servera una implementación integrada, vCenter Server retiene los certificados personalizados. Después de la actualización, el entorno funcionará como antes. Se conservan los certificados existentes de vCenter Server y vCenter Single Sign-On. Los certificados se usan como certificados SSL de equipos. Además, VMCA asigna un certificado firmado por VMCA a cada usuario de solución (recopilación de servicios de vCenter). El usuario de solución utiliza este certificado solo para autenticarse ante vCenter Single Sign-On. VMware no recomienda reemplazar los certificados de usuarios de la solución.

Interfaces de certificados de vSphere

En el caso de vCenter Server, es posible ver y reemplazar certificados con las siguientes herramientas e interfaces.

Tabla 2-3. Interfaces para administrar certificados de vCenter Server

Interfaz	Uso
vSphere Client	Realice tareas de certificados comunes con una interfaz gráfica de usuario.
vSphere Automation API	Consulte la *Guía de programación de VMware vSphere Automation SDK*.
Utilidad vSphere Certificate Manager	Realice tareas de reemplazo de certificados comunes desde la línea de comandos de la instalación de vCenter Server.
CLI de administración de certificados de vSphere	Realice todas las tareas de administración de certificados con `dir-cli`, `certool` y `vecs-cli`.
Utilidad `sso-config`	Realice administración de certificados STS desde la línea de comandos de la instalación de vCenter Server.
PowerCLI 12.4 o versiones posteriores (también requiere vSphere 7.0 o una versión posterior)	Lleve a cabo la administración del almacén de certificados de confianza, administre los certificados SSL de máquina de vCenter Server y administre los certificados SSL de máquina de ESXi.

En el caso de ESXi, puede realizar la administración de certificados desde vSphere Client. VMCA aprovisiona certificados y los almacena localmente en el host ESXi. VMCA no almacena certificados de hosts ESXi en VMDIR o en VECS. Consulte la documentación de *Seguridad de vSphere*.

Certificados admitidos de vCenter Server

En el caso de vCenter Server y las máquinas y los servicios relacionados, se admiten los siguientes certificados:

- Certificados generados y firmados por la entidad de certificación VMware Certificate Authority (VMCA).
- Certificados personalizados.
  - Certificados empresariales que se generan desde su propia PKI interna.
  - Certificados externos firmados por una entidad de certificación que se genera mediante una PKI externa como Verisign, GoDaddy, etc.

No se admiten los certificados autofirmados que se crearon mediante OpenSSL donde no existe una entidad de certificación raíz.

Reemplazar certificados de vSphere

Es posible realizar distintos tipos de reemplazo de certificados según los requisitos y la directiva de la empresa para el sistema que va a configurar. Se pueden reemplazar certificados desde vSphere Client con la utilidad vSphere Certificate Manager o manualmente mediante las CLI que se incluyen con la instalación.

VMware Certificate Authority (VMCA) se incluye en cada implementación de vCenter Server. VMCA aprovisiona cada uno de los nodos, de los usuarios de la solución vCenter Server y de los hosts ESXi con un certificado firmado por VMCA como entidad de certificación.

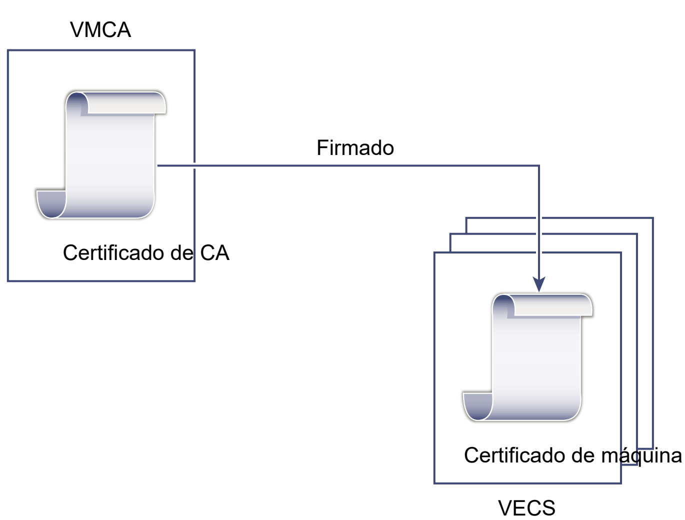
Es posible reemplazar los certificados predeterminados. Para los componentes de vCenter Server, puede usar un conjunto de herramientas de línea de comandos que se incluyen en la instalación. Existen varias opciones.

Nota Si vCenter Server está vinculado a NSX-T Manager y reemplaza los certificados de vCenter Server, debe actualizar la huella digital del administrador de equipos de vCenter Server. Consulte el tema titulado "Agregar un administrador de equipo" en la *Guía del coordinador de migración de NSX-T Data Center*.

Reemplazar certificados por certificados firmados por VMCA

Si su certificado de VMCA vence o si quiere reemplazarlo por otros motivos, puede usar las CLI de administración de certificados para realizar ese proceso. De forma predeterminada, el certificado raíz de VMCA vence después de 10 años y todos los certificados que firma la VMCA vencen cuando caduca el certificado raíz, es decir, después de un máximo de 10 años.

Figura 2-1. Los certificados firmados por VMCA se almacenan en VECS



Puede usar las siguientes opciones de vSphere Certificate Manager:

- Reemplazar un certificado de SSL de una máquina con un certificado de VMCA
- Reemplazo de un certificado de un usuario de una solución con un certificado de VMCA

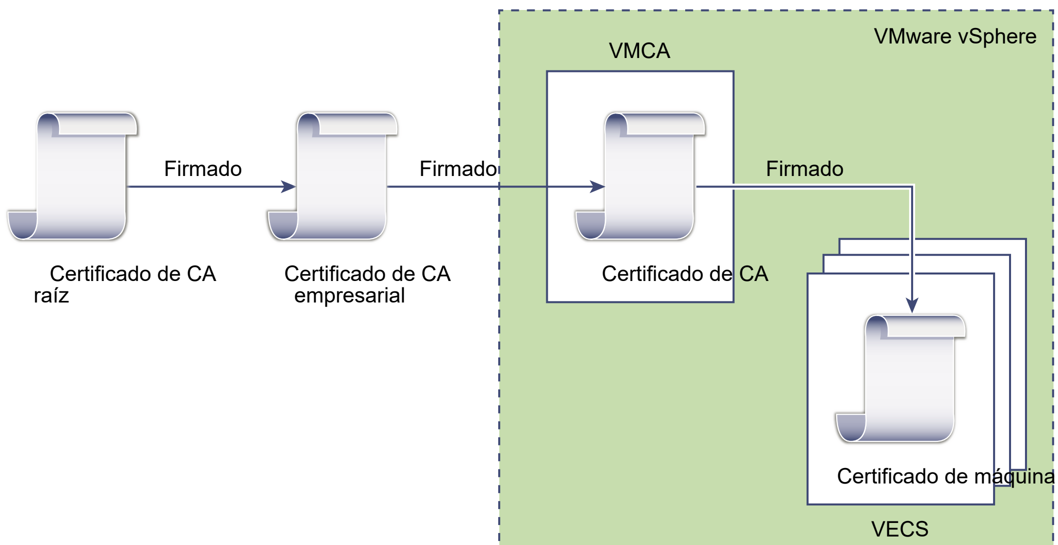
Para obtener información sobre el reemplazo manual de certificados, consulte Reemplazar los certificados firmado por VMCA existentes por certificados nuevos firmados por VMCA mediante la CLI.

Convertir a VMCA en una entidad de certificación intermedia

Puede reemplazar el certificado raíz de VMCA por un certificado firmado por una entidad de certificación (CA) empresarial o de terceros. VMCA firma el certificado raíz cada vez que aprovisiona certificados, lo que convierte a VMCA en una CA intermediaria.

Nota Si realiza una instalación nueva que incluye una instancia de vCenter Server, reemplace el certificado raíz de VMCA antes de agregar hosts ESXi. Si lo hace, VMCA firma toda la cadena y no es necesario generar certificados nuevos.

Figura 2-2. Los certificados firmados por una CA empresarial o externa usan VMCA como CA intermediaria



Puede usar las siguientes opciones de vSphere Certificate Manager:

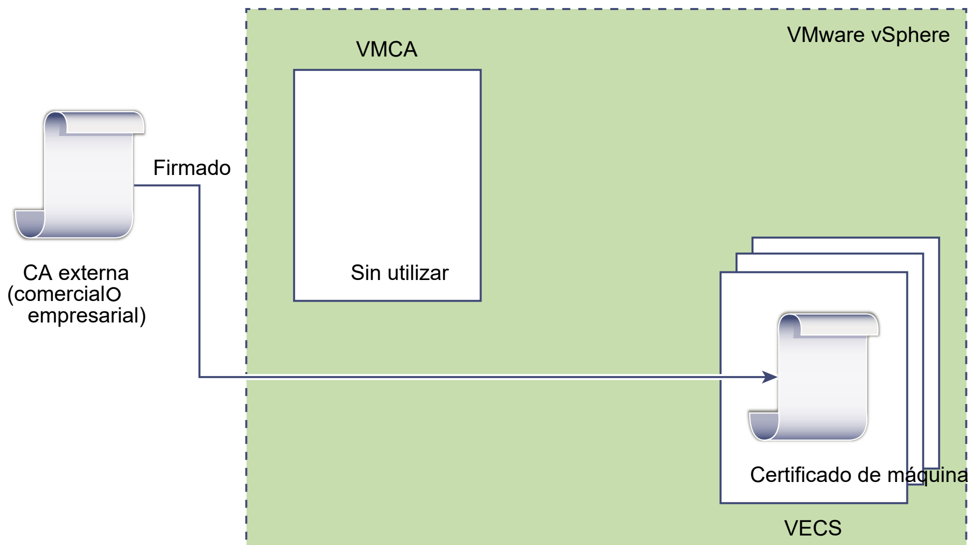
- Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados
- Reemplazar un certificado de SSL de una máquina con un certificado de VMCA (implementación de Enhanced Linked Mode de varios nodos)
- Reemplazar un certificado de usuario de solución con un certificado de VMCA (implementación de Enhanced Linked Mode de varios nodos)

Para obtener información sobre el reemplazo manual de certificados, consulte Convertir VMCA en una entidad de certificación intermedia mediante la CLI.

Reemplazar certificados firmados por VMCA por certificados personalizados

Puede reemplazar los certificados firmados por VMCA existentes con certificados personalizados. Si emplea este enfoque, asume la responsabilidad del aprovisionamiento y la supervisión de todos los certificados.

Figura 2-3. Certificados externos que se almacenan directamente en VECS



Puede usar las siguientes opciones de vSphere Certificate Manager:

- Reemplazar un certificado SSL de máquina por un certificado personalizado
- Reemplazar los certificados de usuarios de soluciones con certificados personalizados

Para obtener información sobre el reemplazo manual de certificados, consulte Reemplazar certificados por certificados personalizados mediante la CLI.

También puede utilizar vSphere Client a fin de generar una CSR para un certificado SSL de máquina (personalizado) y reemplazar el certificado después de que la entidad de certificación lo devuelve. Consulte Generar una solicitud de firma del certificado para el certificado SSL de máquina con vSphere Client (certificados personalizados).

Uso del método híbrido para la implementación de certificados

En el método híbrido, puede hacer que VMCA proporcione algunos de los certificados y, al mismo tiempo, puede usar certificados personalizados para otras partes de la infraestructura. Por ejemplo, dado que los certificados de usuarios de soluciones se usan solo para autenticar vCenter Single Sign-On, considere la posibilidad de hacer que VMCA aprovisione esos certificados. Reemplace los certificados de SSL de máquinas con certificados personalizados para proteger todo el tráfico de SSL.

Con frecuencia, la directiva de la empresa no permite CA intermedias. En esos casos, la implementación híbrida es una buena solución. Minimiza la cantidad de certificados que deben reemplazarse y protege todo el tráfico. La implementación híbrida solo deja tráfico interno, es decir, tráfico del usuario de la solución, para usar los certificados predeterminados firmados por VMCA.

Para obtener más información, consulte la publicación del blog llamada *Revisión del producto nuevo: reemplazo del certificado SSL de vSphere híbrido* en http://vmware.com/go/hybridvmca.

Reemplazar certificados de ESXi

Para los hosts ESXi, puede cambiar el comportamiento de aprovisionamiento de certificados desde vSphere Client. Consulte la documentación de *Seguridad de vSphere* para obtener detalles.

Tabla 2-4. Opciones de reemplazo de certificados de ESXi

Opción	Descripción
Modo VMware Certificate Authority (valor predeterminado)	Cuando se renuevan certificados desde vSphere Client, VMCA emite los certificados para los hosts. Si cambió el certificado raíz de VMCA para incluir una cadena de certificados, los certificados del host incluyen la cadena completa.
Modo de entidad de certificación personalizada	Permite actualizar y usar certificados de forma manual que VMCA no firmó ni emitió.
Modo de huella digital	Puede usarse para conservar los certificados de la versión 5.5 durante la actualización. Use este modo únicamente de manera temporal en situaciones de depuración.

Dónde utiliza certificados vSphere

VMware Certificate Authority (VMCA) aprovisiona su entorno con certificados. Entre ellos se encuentran certificados SSL de equipos para conexiones seguras, certificados de usuarios de solución para la autenticación de servicios ante vCenter Single Sign-On y certificados para hosts ESXi.

Los siguientes certificados están en uso.

Tabla 2-5. Certificados en vSphere

Certificado	Aprovisionado	Comentarios
Certificados de ESXi	VMCA (valor predeterminado)	Almacenados localmente en el host ESXi.
Certificados SSL de máquina	VMCA (valor predeterminado)	Almacenados en el Almacén de certificados de endpoints de VMware (VECS).
Certificados de usuarios de solución	VMCA (valor predeterminado)	Almacenados en VECS.

Tabla 2-5. Certificados en vSphere (continuación)

Certificado	Aprovisionado	Comentarios
Certificado de firma SSL vCenter Single Sign-On	Aprovisionado durante la instalación.	Administre este certificado en la línea de comandos. **Nota** No cambie este certificado en el sistema de archivos, ya que podría producirse un comportamiento impredecible.
Certificado SSL de VMware Directory Service (VMDIR)	Aprovisionado durante la instalación.	En vSphere 6.5 y versiones posteriores, el certificado SSL del equipo se usa como certificado de vmdir.
Certificados autofirmados por SMS	Aprovisionado durante el registro del proveedor de filtro de E/S.	En vSphere 7.0 y versiones posteriores, los certificados autofirmados de SMS se almacenan en `/etc/vmware/ssl/iofiltervp_castore.pem`. Antes de vSphere 7.0, los certificados autofirmados de SMS se almacenan en `/etc/vmware/ssl/castore.pem`. Además, el almacén de SMS también puede almacenar los certificados autofirmados del proveedor VASA de VVOL (versión 4.0 y anteriores) cuando retainVasaProviderCertificate=True.

Certificados de ESXi

Los certificados de ESXi se almacenan localmente en cada host del directorio `/etc/vmware/ssl`. Los certificados de ESXi son aprovisionados por VMCA de manera predeterminada, pero se pueden utilizar certificados personalizados. Los certificados de ESXi se aprovisionan cuando se agrega el host por primera vez a vCenter Server y cuando el host se vuelve a conectar. Para obtener más información, consulte la documentación sobre *Seguridad de vSphere*.

Certificados SSL de máquina

El certificado SSL de máquina de cada nodo se utiliza para crear un socket de SSL en el lado del servidor. Los clientes SSL se conectan con el socket SSL. El certificado se utiliza para comprobar el servidor y establecer una comunicación segura mediante los protocolos HTTPS o LDAPS.

Cada nodo de vCenter Server tiene su propio certificado SSL de máquina. Todos los servicios que se ejecutan en un nodo de vCenter Server utilizan el certificado SSL de máquina para exponer sus endpoints SSL.

Los siguientes servicios utilizan el certificado SSL de máquina.

- El servicio de proxy inverso. Las conexiones SSL a los servicios individuales de vCenter siempre van al proxy inverso. El tráfico no va a los servicios en sí.
- El servicio vCenter Server (vpxd).
- VMware Directory Service (vmdir).

Los productos de VMware utilizan certificados X.509 versión 3 (X.509v3) estándar para cifrar la información de sesión. La información de sesión se envía mediante SSL entre los componentes.

Certificados de usuarios de solución

Un usuario de solución encapsula uno o varios servicios de vCenter Server. Cada usuario de solución debe estar autenticado en vCenter Single Sign-On. Los usuarios de solución utilizan certificados para autenticar vCenter Single Sign-On a través del intercambio de token SAML.

Un usuario de solución presenta el certificado ante vCenter Single Sign-On cuando debe autenticarse por primera vez, después de un reinicio y de transcurrido un tiempo de espera. El tiempo de espera (tiempo de espera Holder-of-Key) puede establecerse desde vSphere Client y su valor predeterminado es 2.592.000 segundos (30 días).

Por ejemplo, el usuario de solución vpxd presenta su certificado en vCenter Single Sign-On al conectarse a vCenter Single Sign-On. El usuario de solución vpxd recibe un token SAML de vCenter Single Sign-On y, a continuación, puede utilizarlo para autenticarse en otros servicios y usuarios de solución.

En VECS, se incluyen los siguientes almacenes de certificados de usuarios de solución:

- `machine`: lo utilizan el servidor de licencias y el servicio de registro.

  Nota El certificado de usuario de solución de la máquina no tiene relación alguna con el certificado SSL de máquina. El certificado de usuario de solución de la máquina se utiliza para el intercambio de tokens SAML, mientras que el certificado SSL de máquina se utiliza para las conexiones SSL seguras de una máquina.

- `vpxd`: almacén de daemon del servicio vCenter (vpxd). vpxd utiliza el certificado de usuario de solución que está almacenado en este almacén para autenticarse en vCenter Single Sign-On.
- `vpxd-extension`: almacén de extensiones de vCenter. Incluye el servicio de Auto Deploy, el servicio de inventario u otros servicios que no forman parte de otros usuarios de solución.
- `vsphere-webclient`: almacén de vSphere Client. También incluye algunos servicios adicionales como el servicio de gráficos de rendimiento.
- `wcp`: VMware vSphere® con almacén de VMware Tanzu™. También se utiliza para vSphere Cluster Services.

Certificados internos

Los certificados de vCenter Single Sign-On no se almacenan en VECS y no se administran con herramientas de administración de certificados. Como regla general, no es necesario hacer cambios, pero en situaciones especiales, estos certificados se pueden reemplazar.

Certificado de firma de vCenter Single Sign-On

El servicio vCenter Single Sign-On incluye un servicio de proveedor de identidad que emite tokens SAML utilizados para la autenticación en todo el sistemavSphere. Un token SAML representa la identidad del usuario y, a su vez, contiene información sobre la pertenencia a los grupos. Cuando vCenter Single Sign-On emite tokens SAML, firma cada token con su certificado de firma, de modo que los clientes de vCenter Single Sign-On pueden comprobar que el token SAML proviene de un origen confiable.

Este certificado se puede reemplazar desde la CLI. Consulte Reemplazar un certificado vCenter Server STS mediante la línea de comandos.

Certificado SSL de VMware Directory Service

En vSphere 6.5 y versiones posteriores, el certificado SSL del equipo se usa como certificado de directorio VMware. Para versiones anteriores de vSphere, consulte la documentación correspondiente.

vSphereCertificados de cifrado de máquinas virtuales

La solución vSphere cifrado de máquinas virtuales se conecta con un servidor de claves. Según la manera en que la solución se autentique ante el servidor de claves, puede generar certificados y almacenarlos en VECS. Consulte la documentación de *Seguridad de vSphere*.

VMware Certificate Authority y Servicios básicos de identidad VMware

Los servicios básicos de identidad forman parte de cada sistema vCenter Server. VMware Certificate Authority (VMCA) forma parte de cada grupo de servicios de identidad principal de VMware. Utilice las CLI de administración y vSphere Client para interactuar con estos servicios.

Los servicios básicos de identidad de VMware incluyen varios componentes.

Tabla 2-6. Servicios básicos de identidad

Servicio	Descripción
VMware Directory Service (vmdir)	Origen de identidad que controla la administración de certificados SAML para la autenticación con vCenter Single Sign-On.
VMware Certificate Authority (VMCA)	Emite certificados para usuarios de soluciones de VMware, certificados para las máquinas en las que se ejecutan servicios y certificados para hosts ESXi. VMCA puede utilizarse en el estado en que se encuentra o como entidad de certificación intermediaria. VMCA emite certificaciones únicamente a los clientes que pueden autenticarse en vCenter Single Sign-On en el mismo dominio.
VMware Authentication Framework Daemon (VMAFD)	Incluye VMware Endpoint Certificate Store (VECS) y otros servicios de autenticación. Los administradores de VMware interactúan con VECS; los otros servicios son de uso interno.

VMware Endpoint Certificate Store

VMware Endpoint Certificate Store (VECS) sirve de repositorio local (del lado del cliente) para certificados, claves privadas y cualquier información de certificados que pueda guardarse en un

almacén de claves. Puede optar por no usar VMCA como entidad de certificación y firmante de certificados, pero debe usarlo para almacenar todos los certificados, las claves y demás elementos de vCenter. Los certificados de ESXi se almacenan de forma local en cada host y no en VECS.

VECS se ejecuta como parte de VMware Authentication Framework Daemon (VMAFD). VECS se ejecuta en cada nodo de vCenter Server y conserva todos los almacenes de claves que contienen certificados y claves.

VECS sondea VMware Directory Service (vmdir) de forma periódica en busca de actualizaciones del almacén raíz de confianza. También puede administrar certificados de forma explícita en VECS mediante los comandos `vecs-cli`. Consulte Referencia de comandos vecs-cli.

VECS incluye los siguientes almacenes.

Tabla 2-7. Almacenes en VECS

Almacén	Descripción
Almacén SSL de máquina (MACHINE_SSL_CERT)	■ El servicio de proxy inverso lo utiliza en cada nodo de vSphere. ■ VMware Directory Service (vmdir) lo utiliza en cada nodo de vCenter Server. Todos los servicios de vSphere 6.0 y versiones posteriores se comunican mediante un proxy inverso que utiliza el certificado SSL de equipo. Por razones de compatibilidad con versiones anteriores, los servicios de la versión 5.x todavía utilizan puertos específicos. Como resultado, algunos servicios como vpxd todavía tienen su propio puerto abierto.
Almacenes de usuarios de solución ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	VECS incluye un almacén para cada usuario de solución. El asunto de cada certificado de usuario de solución debe ser único, por ejemplo, el certificado de máquina no puede tener el mismo asunto que el certificado de vpxd. Los certificados de usuarios de solución se utilizan para efectuar la autenticación con vCenter Single Sign-On. vCenter Single Sign-On comprueba que el certificado sea válido, pero no comprueba otros atributos del certificado. En VECS, se incluyen los siguientes almacenes de certificados de usuarios de solución: ■ `machine`: lo utilizan el servidor de licencias y el servicio de registro. **Nota** El certificado de usuario de solución de la máquina no tiene relación alguna con el certificado SSL de máquina. El certificado de usuario de solución de la máquina se utiliza para el intercambio de tokens SAML, mientras que el certificado SSL de máquina se utiliza para las conexiones SSL seguras de una máquina. ■ `vpxd`: almacén de daemon del servicio vCenter (vpxd). vpxd utiliza el certificado de usuario de solución que está almacenado en este almacén para autenticarse en vCenter Single Sign-On. ■ `vpxd-extension`: almacén de extensiones de vCenter. Incluye el servicio de Auto Deploy, el servicio de inventario u otros servicios que no forman parte de otros usuarios de solución. ■ `vsphere-webclient`: almacén de vSphere Client. También incluye algunos servicios adicionales como el servicio de gráficos de rendimiento. ■ `wcp`: VMware vSphere® con almacén de VMware Tanzu™. También se utiliza para vSphere Cluster Services. Cada nodo de vCenter Server incluye un certificado `machine`.
Almacén raíz de confianza (TRUSTED_ROOTS)	Contiene todos los certificados raíz de confianza.

Tabla 2-7. Almacenes en VECS (continuación)

Almacén	Descripción
Almacén de copias de seguridad de la utilidad vSphere Certificate Manager (BACKUP_STORE)	VMCA (VMware Certificate Manager) lo utiliza para admitir la reversión de certificados. Solo el estado más reciente se almacena como copia de seguridad; no se puede volver más de un paso.
Otros almacenes	Las soluciones pueden agregar otros almacenes. Por ejemplo, la solución Virtual Volumes agrega un almacén SMS. No modifique los certificados de estos almacenes a menos que así se indique en la documentación de VMware o en un artículo de la base de conocimientos de VMware. **Nota** La eliminación del almacén TRUSTED_ROOTS_CRLS puede dañar la infraestructura de certificado. No elimine ni modifique el almacén TRUSTED_ROOTS_CRLS.

El servicio de vCenter Single Sign-On almacena el certificado de firma de tokens y su certificado SSL en el disco. Puede cambiar el certificado de firma de tokens desde la CLI.

Algunos certificados se almacenan en el sistema de archivos, ya sea de forma temporal durante el inicio o de forma permanente. No cambie los certificados en el sistema de archivos.

Nota No cambie ningún archivo de certificado en el disco a menos que se indique en la documentación de VMware o en los artículos de la base de conocimientos. De lo contrario, se puede producir un comportamiento inesperado.

Administrar la revocación de certificados de vSphere

Si sospecha que la confiabilidad de uno de los certificados está comprometida, reemplace todos los certificados actuales, incluido el certificado raíz de VMCA.

vSphere admite el reemplazo de los certificados, pero no aplica su revocación en los hosts ESXi ni en los sistemas vCenter Server.

Quite los certificados revocados de todos los nodos. Si no los quita, un ataque de tipo "Man in the middle" podría comprometerlos al habilitarse una suplantación con las credenciales de la cuenta.

Reemplazar certificados de vSphere en implementaciones grandes

Al reemplazar certificados en implementaciones con un gran número de hosts vCenter Server, se puede utilizar la utilidad de administración de certificados de vSphere o reemplazar los certificados de forma manual con las CLI. Algunas prácticas recomendadas dirigen el proceso que elija.

Reemplazar certificados SSL de máquina en entornos con varios sistemas vCenter Server

Si el entorno incluye varios sistemas vCenter Server, puede reemplazar los certificados SSL de máquina mediante vSphere Client o la utilidad vSphere Certificate Manager, o bien hacerlo manualmente con comandos CLI.

Usar vSphere Certificate Manager para reemplazar certificados SSL de máquina en varios sistemas vCenter Server

Ejecute vSphere Certificate Manager en cada máquina. Según la tarea que realice, también se le solicitará información del certificado. Consulte los siguientes temas para obtener más detalles:

- Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados mediante el Certificate Manager
- Reemplazar un certificado SSL de máquina por un certificado de VMCA (entidad de certificación intermedia) mediante Certificate Manager
- Reemplazar certificados de usuario de solución por certificados de VMCA (entidad de certificación intermedia) mediante Certificate Manager

Usar la CLI para reemplazar manualmente certificados SSL de máquina en varios sistemas vCenter Server

Para reemplazar un certificado manualmente, ejecute los comandos CLI de reemplazo de los certificados en cada máquina. Consulte los siguientes temas para obtener más detalles:

- Reemplazar los certificados SSL de máquina por certificados firmados por VMCA mediante la CLI
- Reemplazar certificados SSL de máquina (entidad de certificación intermedia) mediante la CLI
- Reemplazar certificados SSL de máquina por certificados personalizados mediante la CLI

Reemplazar certificados de usuarios de solución en entornos con varios sistemas vCenter Server en Enhanced Linked Mode

Si el entorno incluye varios sistemas vCenter Server en Enhanced Linked Mode, siga estos pasos para reemplazar certificados de usuario de solución.

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `/usr/lib/vmware-vmafd/bin/dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

Usar vSphere Certificate Manager para reemplazar certificados SSL de máquina en sistemas vCenter Server en ELM

Ejecute vSphere Certificate Manager en cada máquina. Según la tarea que realice, también se le solicitará información del certificado. Consulte Administrar certificados mediante la utilidad de vSphere Certificate Manager.

Usar la CLI para reemplazar manualmente certificados SSL de máquina en sistemas vCenter Server en ELM

Los pasos detallados para reemplazar manualmente certificados SSL de máquina en vCenter Server en ELM son los siguientes:

1 Generar o solicitar un certificado.

   Necesita los siguientes certificados:

   - Un certificado para el usuario de solución de la máquina en cada instancia de vCenter Server.
   - Un certificado para cada uno de los siguientes usuarios de solución en cada nodo:
     - usuario de la solución `vpxd`
     - usuario de la solución `vpxd-extension`
     - usuario de la solución `vsphere-webclient`
     - usuario de la solución `wcp`

2 Utilice los comandos de la CLI para reemplazar los certificados en cada nodo.

   El proceso en particular depende del tipo de reemplazo de certificados que esté realizando. Consulte los siguientes temas para obtener más detalles:

   - Reemplazar los certificados de usuarios de solución por certificados nuevos firmados por VMCA mediante la CLI
   - Reemplazar certificados de usuario de solución (entidad de certificación intermedia) mediante la CLI
   - Reemplazar certificados de usuario de solución por certificados personalizados mediante el administrador de certificados

Reemplazo de certificados en entornos de VMware que incluyen soluciones externas

Algunas soluciones, como VMware vCenter Site Recovery Manager o VMware vSphere Replication, siempre se instalan en una máquina distinta del sistema vCenter Server. Si se reemplaza el certificado SSL de máquina predeterminado en el sistema vCenter Server, se produce un error de conexión cuando la solución intenta conectarse al sistema vCenter Server.

Es posible ejecutar el script `ls_update_certs` para solucionar el problema. Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2109074.

Administrar certificados mediante el vSphere Client

Puede ver y administrar certificados mediante vSphere Client.

vSphere Client le permite realizar estas tareas de administración.

- Vea los certificados SSL, raíz de VMware Certificate Authority (VMCA), raíz de confianza y servicio de token de seguridad (STS) de máquina.
- Agregue nuevos certificados raíz de confianza y renueve o reemplace los certificados SSL y STS de máquina existentes.
- Generar una solicitud de firma del certificado (Certificate Signing Request, CSR) personalizada para un certificado SSL de máquina y reemplazar el certificado cuando la entidad de certificación lo devuelva.

La mayor parte de los flujos de trabajo de reemplazo de certificados se admite completamente desde vSphere Client. La utilidad vSphere Certificate Manager admite otros flujos de trabajo de reemplazo de certificados. Consulte Administrar certificados mediante la utilidad de vSphere Certificate Manager.

Para obtener más información sobre las opciones para reemplazar los certificados predeterminados, consulte Reemplazar certificados de vSphere.

Nota Si utiliza el VMCA como una entidad de certificación intermedia o utiliza certificados personalizados, es posible que experimente una complejidad considerable y que exista la posibilidad de un impacto negativo para la seguridad, así como un aumento innecesario en el riesgo operativo. Para obtener más información sobre la administración de certificados en un entorno de vSphere, consulte la publicación de blog llamada *Revisión de producto nuevo: reemplazo del certificado SSL de vSphere híbrido* en http://vmware.com/go/hybridvmca.

Explorar los almacenes de certificados mediante vSphere Client

En cada nodo de vCenter Server, se incluye una instancia de VMware Endpoint Certificate Store (VECS). Puede explorar los diferentes almacenes dentro del almacén de certificados de endpoint de VMware desde vSphere Client, incluidos los certificados SSL de máquina, STS y raíz de confianza.

Consulte VMware Endpoint Certificate Store para obtener detalles sobre los diferentes almacenes incluidos en VECS.

Requisitos previos

Para la mayoría de las tareas de administración, debe contar con la contraseña del administrador de la cuenta de dominio local, administrator@vsphere.local o un dominio diferente si cambió el dominio durante la instalación.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Si el sistema lo solicita, introduzca las credenciales de su instancia de vCenter Server.

5 Explore los certificados almacenados en VMware Endpoint Certificate Store (VECS).

   VMware Endpoint Certificate Store explica qué hay en los almacenes individuales.

6 Para ver los detalles de un certificado, seleccione la pestaña de certificados correspondiente, seleccione el certificado y amplíe el certificado para ver los detalles.

Establecer el umbral para las advertencias de caducidad de certificados de vCenter mediante vSphere Client

vCenter Server supervisa todos los certificados de VMware Endpoint Certificate Store (VECS) y emite una alarma cuando un certificado está a 30 días o menos de caducar. Puede usar el vSphere Client para cambiar la anticipación con la que desea recibir el alerta con la opción avanzada `vpxd.cert.threshold`.

Procedimiento

1 Inicie sesión en vSphere Client.

2 Seleccione el objeto vCenter Server y haga clic en **Configurar**.

3 Haga clic en **Configuración avanzada**.

4 Haga clic en **Editar configuración** y filtre por **`umbral`**.

5 Cambie la configuración de `vpxd.cert.threshold` al valor deseado y haga clic en **Guardar**.

Reemplazar certificados de VMCA por nuevos certificados firmados por VMCA con vSphere Client

Todos los certificados firmados por VMCA se pueden reemplazar por nuevos certificados firmados por VMCA. Este proceso se denomina "renovación de certificados". Puede renovar los certificados seleccionados o todos los certificados del entorno desde vSphere Client.

Requisitos previos

Para la administración de certificados, debe proporcionar la contraseña del administrador del dominio local (administrator@vsphere.local de forma predeterminada). Si está renovando certificados para un sistema vCenter Server, también puede proporcionar las credenciales de vCenter Single Sign-On para un usuario con privilegios de administrador en el sistema vCenter Server.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Si el sistema lo solicita, introduzca las credenciales de su instancia de vCenter Server.

5 Renueve el certificado SSL de máquina firmado por VMCA para el sistema local.

   a En la pestaña **SSL de máquina**, seleccione el certificado que desee y haga clic en**Renovar**.

   b Especifique la duración del certificado en días.

   c Haga clic en la casilla de verificación para confirmar que ha realizado una copia de seguridad de vCenter Server y sus bases de datos.

   d Haga clic en **Renovar**.

      El sistema renueva el certificado y muestra un mensaje de operación correcta.

   e Cuando aparezca el mensaje de que se cambió el certificado, haga clic en **Actualizar** para actualizar el navegador.

Reemplazar certificados por certificados personalizados mediante vSphere Client

Puede utilizar vSphere Client para reemplazar los certificados predeterminados por certificados personalizados.

Puede utilizar el vSphere Client para generar CSR para cada máquina y reemplazar los certificados cuando los reciba de la entidad de certificación (CA) interna o externa. Cuando entrega las CSR a su CA interna o externa, la CA devuelve certificados firmados y el certificado raíz. Se puede cargar el certificado raíz y los certificados firmados desde la vSphere Client.

Generar una solicitud de firma del certificado para el certificado SSL de máquina con vSphere Client (certificados personalizados)

El certificado SSL de máquina se utiliza en el servicio de proxy inverso de cada nodo de vCenter Server. Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. Puede utilizar vSphere Client para generar una solicitud de firma del certificado (CSR) para el certificado SSL de máquina y reemplazar el certificado una vez que esté listo.

Requisitos previos

El certificado debe cumplir con los siguientes requisitos:

- Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM). vSphere Client y la API siguen aceptando un tamaño de clave de hasta 16.384 bits al generar la solicitud de firma del certificado.
- Formato CRT
- x509 versión 3
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Contiene los siguientes usos de claves: firma digital, cifrado de clave

---

Nota El certificado FIPS de vSphere solo valida los tamaños de clave RSA de 2048 y 3072 bits.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Introduzca las credenciales de vCenter Server.

5 Genere la CSR.

   a En la pestaña **SSL de máquina**, seleccione el certificado deseado y haga clic en **Generar solicitud de firma del certificado (CSR)**.

   b Introduzca la información del certificado y haga clic en **Siguiente**.

   2048 (bits) es el valor predeterminado para el tamaño de clave. Cambie este valor según sea necesario.

   Nota Cuando se utiliza vCenter Server para generar una CSR con un tamaño de clave grande, la generación tarda unos minutos en completarse debido a la naturaleza de la operación que requiere un uso intensivo de la CPU.

   ---

   c Copie o descargue la CSR.

   d Haga clic en **Finalizar**.

   e Proporcione la CSR a su entidad de certificación.

Pasos siguientes

Cuando la entidad de certificación devuelve el certificado, reemplace el certificado existente en el almacén de certificados. Consulte Agregar certificados personalizados mediante vSphere Client.

Agregar un certificado raíz de confianza al almacén de certificados mediante vSphere Client

Si desea utilizar certificados de terceros en su entorno, debe agregar un certificado raíz de confianza al almacén de certificados. Puede hacerlo mediante vSphere Client.

Requisitos previos

Obtenga el certificado raíz personalizado de la entidad de certificación (CA) interna o de terceros.

vSphere solo acepta certificados de CA válidos para la importación. Para que sea válido, un certificado de CA debe tener el bit de CA y el bit keyCertSign establecidos en la restricción básica y las extensiones de certificado X.509 v3 de uso de clave, respectivamente. Esto implica que el certificado sea de CA y su finalidad sea la firma de certificados. Consulte https://www.rfc-editor.org/rfc/rfc5280 para obtener más información.

Asegúrese de que el bit keyCertSign esté establecido para todos los certificados de la cadena.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Si el sistema lo solicita, introduzca las credenciales de su instancia de vCenter Server.

5 En la pestaña **Raíz de confianza**, haga clic en **Agregar certificado raíz de confianza**.

6 Haga clic en **Examinar** y seleccione la ubicación de la cadena de certificados.

   Puede usar un archivo del tipo CER, PEM o CRT.

7 Haga clic en **Agregar**.

El certificado se agrega al almacén.

Nota En vSphere 8.0 Update 2 y otras versiones posteriores, se elimina la casilla de verificación **Iniciar inserción de certificado raíz en hosts de vCenter**. vCenter Server inserta los certificados raíz en todos los hosts conectados del inventario cuando se agrega un certificado. Cuando se conecta un host con certificados raíz diferentes de vCenter Server, vCenter Server inserta los certificados raíz para corregir esta diferencia. En este caso, los certificados raíz de vCenter Server sobrescriben los del host para que los administradores puedan asegurarse de que los certificados raíz personalizados necesarios en todo el inventario se agreguen a vCenter Server.

Agregar certificados personalizados mediante vSphere Client

Puede utilizar vSphere Client para agregar certificados SSL de máquina personalizados al almacén de certificados.

Por lo general, reemplazar el certificado SSL de máquina para cada componente es suficiente.

Requisitos previos

Genere solicitudes de firma de certificado (Certificate Signing Requests, CSR) para cada certificado que desea reemplazar. Consulte Generar una solicitud de firma del certificado para el certificado SSL de máquina con vSphere Client (certificados personalizados). Coloque el certificado y la clave privada en una ubicación accesible para vCenter Server.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Si el sistema lo solicita, introduzca las credenciales de su instancia de vCenter Server.

5 En la pestaña **SSL de máquina**, seleccione el certificado y, a continuación, haga clic en **Importar y reemplazar certificado**.

6 Haga clic en la opción de reemplazo de certificados adecuada y, a continuación, haga clic en **Siguiente**.

Opción	Descripción
Reemplazar con un certificado de VMCA	Crea una CSR generada por VMCA para reemplazar el certificado actual.
Reemplazar con un certificado de CA externa en el que se genera una CSR a partir de vCenter Server (clave privada integrada)	Utilice un certificado firmado mediante una CSR generada por vCenter Server para reemplazar el certificado actual.
Reemplazar con un certificado de entidad de certificación externa (requiere clave privada)	Utilice un certificado firmado por una entidad de certificación externa para reemplazar el certificado actual.

7 Introduzca la información de CSR o cargue los certificados apropiados.

8 Haga clic en la casilla de verificación para confirmar que ha realizado una copia de seguridad de vCenter Server y sus bases de datos.

9 Revise la información y haga clic en **Finalizar**.

   El sistema reemplaza el certificado y muestra un mensaje de operación correcta.

10 Cuando aparezca el mensaje de que se cambió el certificado, haga clic en **Actualizar** para actualizar el navegador.

Generar un certificado de hoja de VMCA

Es posible generar un certificado de hoja firmado por VMware Certificate Authority (VMCA) para usarlo en la infraestructura de VMware.

Además de VMware Certificate Authority (VMCA) que se ocupa de toda la administración de certificados, puede generar certificados de hoja. VMCA firma los certificados de hoja y estos se utilizan para identificar otros recursos de VMware. Los certificados de hoja generados por VMCA no se almacenan en VECS. Además, vCenter Server no realiza un seguimiento de estos certificados de hoja para comprobar su caducidad.

Requisitos previos

Genere una solicitud de firma del certificado (Certificate Signing Request, CSR) en el host de la infraestructura de VMware en la que desea instalar el certificado de hoja.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Si el sistema lo solicita, introduzca las credenciales de su instancia de vCenter Server.

5 En la pestaña **Raíz de confianza**, seleccione el certificado raíz de VMCA y haga clic en **Emitir nuevo certificado de hoja**.

6 Busque la CSR que generó anteriormente, especifique una duración y, a continuación, haga clic en **Siguiente**.

7 Haga clic en **Descargar certificados** para guardar los certificados raíz y de hoja.

Resultados

Los certificados raíz y de hoja generados se crean y se descargan en la ubicación especificada.

Pasos siguientes

Importe los certificados raíz y de hoja en el host de destino de su infraestructura de VMware.

Administrar certificados mediante la utilidad de vSphere Certificate Manager

La utilidad vSphere Certificate Manager permite realizar la mayoría de las tareas de administración de certificados de forma interactiva desde la línea de comandos. vSphere Certificate Manager solicita que se lleve a cabo una tarea, pide las ubicaciones de los certificados y otra información necesaria y, a continuación, detiene e inicia los servicios para reemplazar los certificados.

Para obtener más información sobre las opciones para reemplazar los certificados predeterminados, consulte Reemplazar certificados de vSphere.

Nota Si utiliza el VMCA como una entidad de certificación intermedia o utiliza certificados personalizados, es posible que experimente una complejidad considerable y que exista la posibilidad de un impacto negativo para la seguridad, así como un aumento innecesario en el riesgo operativo. Para obtener más información sobre la administración de certificados en un entorno de vSphere, consulte la publicación de blog llamada *Revisión de producto nuevo: reemplazo del certificado SSL de vSphere híbrido* en http://vmware.com/go/hybridvmca.

Si se utiliza vSphere Certificate Manager, el usuario no es responsable de colocar los certificados en VECS (VMware Endpoint Certificate Store) ni de iniciar y detener los servicios.

Puede ejecutar las opciones de vSphere Certificate Manager en secuencia para completar un flujo de trabajo. Varias opciones, como la generación de CSR, se utilizan en distintos flujos de trabajo. Antes de ejecutar vSphere Certificate Manager, asegúrese de comprender el proceso de reemplazo y consiga los certificados que desea utilizar.

Precaución vSphere Certificate Manager admite un nivel de reversión. Si se ejecuta vSphere Certificate Manager dos veces y se observa que el entorno se dañó de forma inesperada, la herramienta no puede revertir la primera de las dos ejecuciones.

Ubicación de la utilidad de vSphere Certificate Manager

La utilidad vSphere Certificate Manager se encuentra en:

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

Nota Al ejecutar vSphere Certificate Manager, algunas opciones le solicitan lo siguiente:

```
Enter proper value for VMCA 'Name':
```

Responda a este mensaje introduciendo el nombre de dominio completo de la máquina en la que se ejecuta la configuración del certificado.

Flujos de trabajo de la utilidad de vSphere Certificate Manager

La siguiente tabla presenta una descripción general de los flujos de trabajo de reemplazo de certificados que puede realizar mediante la utilidad vSphere Certificate Manager.

Tabla 2-8. Flujos de trabajo de la utilidad de administración de certificados de vSphere

Flujo de trabajo	Descripción	Consulte
Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados	Para generar el certificado raíz de VMCA y reemplazar todos los certificados, utilice la opción 4, vuelva a generar un nuevo certificado raíz de VMCA y reemplace todos los certificados.	Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados con el Certificate Manager
Convertir a VMCA en una entidad de certificación intermedia	Para que VMCA sea una CA intermedia, debe ejecutar la utilidad vSphere Certificate Manager varias veces y usar varias opciones. Este flujo de trabajo ofrece el conjunto completo de pasos para reemplazar los certificados SSL de máquina y los certificados de usuarios de soluciones.	Convertir a VMCA en una entidad de certificación intermedia mediante Certificate Manager

Tabla 2-8. Flujos de trabajo de la utilidad de administración de certificados de vSphere (continuación)

Flujo de trabajo	Descripción	Consulte
Reemplazar todos los certificados por certificados personalizados	Para reemplazar todos los certificados por certificados personalizados debe ejecutar la utilidad vSphere Certificate Manager varias veces y usar varias opciones. Este flujo de trabajo ofrece el conjunto completo de pasos para reemplazar los certificados SSL de máquina y los certificados de usuarios de soluciones.	Reemplazar todos los certificados por certificados personalizados con el Certificate Manager
Revirtiendo la última operación realizada	Para revertir la última operación de certificado realizada y volver al estado anterior. Utilice la opción 7. Revertir la última operación realizada volviendo a publicar los certificados antiguos.	Revertir la última operación realizada al volver a publicar certificados antiguos mediante el administrador de certificados
Restableciendo todos los certificados	Para reemplazar todos los certificados de vCenter existentes por certificados firmados por VMCA, utilice la opción 8 Restablecer todos los certificados.	Restablecer todos los certificados mediante Certificate Manager

Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados con el Certificate Manager

Puede usar la utilidad vSphere Certificate Manager para volver a generar el certificado raíz de VMCA para reemplazar el certificado SSL de máquina local, y reemplazar los certificados de usuarios de soluciones locales por certificados firmados por VMCA. Cuando varias instancias de vCenter Server están conectadas en la configuración de Enhanced Linked Mode, debe reemplazar los certificados en cada vCenter Server.

Al reemplazar el certificado SSL de máquina existente por un nuevo certificado firmado por VMCA, vSphere Certificate Manager solicita información e introduce todos los valores, excepto la contraseña y la dirección IP de vCenter Server, en el archivo `certool.cfg`.

- Contraseña de administrator@vsphere.local
- Código de país de dos letras
- Nombre de empresa
- Nombre de organización
- Unidad de organización
- Estado
- Localidad

- Dirección IP (opcional)
- Correo electrónico
- Nombre del host, es decir, el nombre de dominio completo de la máquina para la que se desea reemplazar el certificado. Si el nombre del host no coincide con el FQDN, el reemplazo de los certificados no se completa correctamente y el entorno puede quedar en un estado inestable.
- Dirección IP de vCenter Server
- Nombre de VMCA, es decir, el nombre de dominio completo de la máquina en la que se ejecuta la configuración del certificado.

Nota El campo OU (organizationalUnitName) ya no es obligatorio.

Requisitos previos

Cuando se ejecuta vSphere Certificate Manager con esta opción, se necesita la siguiente información.

- Contraseña de administrator@vsphere.local.
- FQDN de la máquina para la cual se desea generar un nuevo certificado firmado por VMCA. Las demás propiedades tienen los valores predeterminados, pero pueden cambiarse.

Procedimiento

1 Inicie sesión en el shell de vCenter Server e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Seleccione la opción 4 Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados.

3 Escriba el nombre de usuario y la contraseña del administrador.

4 Responda las solicitudes del sistema.

   vSphere Certificate Manager generará un nuevo certificado raíz de VMCA en función de su entrada y reemplazará todos los certificados en el sistema donde se ejecuta vSphere Certificate Manager. El proceso de sustitución se completa después de que vSphere Certificate Manager haya reiniciado los servicios.

5 Para reemplazar el certificado SSL de máquina, ejecute vSphere Certificate Manager con la opción 3, Reemplazar el certificado SSL de máquina por un certificado de VMCA.

6 Para reemplazar los certificados de usuarios de solución, ejecute Certificate Manager con la opción 6, Reemplazar certificados de usuario de solución por certificados de VMCA.

Convertir a VMCA en una entidad de certificación intermedia mediante Certificate Manager

Puede utilizar la utilidad vSphere Certificate Manager para convertir a VMCA en una entidad de certificación intermedia. Una vez completado el proceso, VMCA firmará todos los certificados nuevos con la cadena completa. Si lo desea, puede utilizar vSphere Certificate Manager para reemplazar todos los certificados existentes por nuevos certificados firmados por VMCA.

Para convertir a VMCA en una CA intermedia, debe ejecutar vSphere Certificate Manager varias veces. Los pasos de alto nivel para reemplazar los certificados SSL de máquina y los certificados de usuarios de solución incluyen:

1. Iniciando la utilidad vSphere Certificate Manager.
2. Generar una CSR mediante la ejecución de la opción 2, Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados. A continuación, debe introducir algunos datos sobre el certificado. Cuando se le pida que elija de nuevo una opción, seleccione Opción 1, Generar solicitudes de firma de certificado y claves para el certificado de firma raíz de VMCA.
3. Envíe la CSR a la CA externa o de la empresa. Recibirá un certificado firmado y un certificado raíz de la CA.
4. Combinar el certificado raíz de VMCA con el certificado raíz de CA y guardar el archivo.
5. Reemplazar certificados mediante la ejecución de la opción 2, Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado, reemplazar todos los certificados y seguir las indicaciones. Este proceso reemplaza todos los certificados en el equipo local.
6. (Opcional) Reemplazar certificados en cada nodo cuando varias instancias de vCenter Server están conectadas en la configuración de Enhanced Linked Mode haciendo lo siguiente:
   a. En primer lugar, reemplace el certificado SSL de máquina por el (nuevo) certificado de VMCA (opción 3, Reemplazar certificados SSL de máquina por certificados de VMCA).
   b. A continuación, reemplace los certificados de usuarios de solución por el (nuevo) certificado de VMCA (opción 6, Reemplazar certificados de usuarios de solución por certificados de VMCA).

Generar una CSR con Certificate Manager y preparar certificados raíz (CA intermedia)

La utilidad vSphere Certificate Manager se puede utilizar para generar solicitudes de firma del certificado (CSR). Envíe esas CSR a la CA de la empresa o a una entidad de certificación externa

para su firma. Los certificados firmados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

- Se puede utilizar vSphere Certificate Manager para crear la CSR.

  Nota A partir de vSphere 8.0 y otras versiones posteriores, si utiliza vSphere Certificate Manager para generar la CSR, el tamaño mínimo de la clave pasa de 2048 bits a 3072 bits. En vSphere 8.0 Update 1 y versiones posteriores, utilice vSphere Client para generar una CSR con un tamaño de clave de 2048 bits.

  Nota El certificado FIPS de vSphere solo valida los tamaños de clave RSA de 2048 y 3072 bits.

- Si prefiere crear la CSR de forma manual, el certificado que envíe para firmar debe cumplir con los siguientes requisitos.
  - Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
  - Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
  - x509 versión 3
  - Para certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos. Por ejemplo:

    ```
    basicConstraints        = critical,CA:true
    keyUsage                = critical,digitalSignature,keyCertSign
    ```

  - La firma CRL debe estar habilitada.
  - Uso mejorado de clave puede estar vacío o contener autenticación del servidor.
  - No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados.
  - No se admiten los certificados con comodines o con más de un nombre DNS.
  - No se pueden crear CA subsidiarias de VMCA.

    Para obtener un ejemplo de uso de la entidad de certificación de Microsoft, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2112009, Crear una plantilla de entidad de certificación de Microsoft para creación de certificados SSL en vSphere 6.x.

Requisitos previos

vSphere Certificate Manager solicita información. Las solicitudes dependen del entorno y del tipo de certificado que se desea reemplazar.

Para cualquier tipo de generación de CSR, se solicita la contraseña del usuario administrator@vsphere.local o el administrador del dominio de vCenter Single Sign-On con el que se desea establecer la conexión.

Procedimiento

1 Inicie sesión en el shell de vCenter Server e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Seleccione la opción 2, Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados.

Inicialmente, esta opción se utiliza para generar la CSR, no para reemplazar los certificados.

3 Escriba el nombre de usuario y la contraseña del administrador.

4 Seleccione la opción 1, Generar solicitudes de firma de certificado y claves para el certificado de firma raíz de VMCA, si desea generar la CSR y seguir las indicaciones.

Es necesario especificar un directorio como parte de este proceso. vSphere Certificate Manager coloca el certificado que se va a firmar (archivo `*.csr`) y el archivo de clave correspondiente (archivo `*.key`) en el directorio.

5 Otorgue un nombre a la solicitud de firma del certificado (Certificate Signing Request, CSR) `root_signing_cert.csr`.

6 Envíe la CSR a la empresa o a la CA externa para firmarla y asigne un nombre al certificado firmado `root_signing_cert.cer` resultante.

7 En un editor de texto, combine el certificado de la siguiente manera.

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

8 Guarde el archivo como `root_signing_chain.cer`.

Pasos siguientes

Reemplace el certificado raíz existente por el certificado raíz en cadena. Consulte Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados mediante el Certificate Manager.

Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados mediante el Certificate Manager

Puede utilizar la utilidad vSphere Certificate Manager para generar una solicitud de firma de certificados (Certificate Signing Requests, CSR) y enviarla a una entidad de certificación de la empresa o de terceros para la firma. A continuación, puede reemplazar el certificado raíz de

VMCA por un certificado de firma personalizado y reemplazar todos los certificados existentes por certificados firmados por la entidad de certificación personalizada.

vSphere Certificate Manager se ejecuta en vCenter Server para reemplazar el certificado raíz de VMCA por un certificado de firma personalizado.

Requisitos previos

- Genere la cadena de certificados.
  - Se puede utilizar vSphere Certificate Manager para crear la solicitud CSR o crear manualmente la CSR.
  - Después de recibir el certificado firmado de la entidad de certificación externa o empresarial, combínelo con el certificado raíz de VMCA inicial para crear la cadena completa.

    Consulte Generar una CSR con Certificate Manager y preparar certificados raíz (CA intermedia) para conocer los requisitos de certificación y el proceso para combinar los certificados.
- Recopile la información que necesita.
  - Contraseña de administrator@vsphere.local
  - Un certificado personalizado válido para la raíz (archivo `.crt`)
  - Clave personalizada válida para la raíz (archivo `.key`)

Procedimiento

1 Inicie sesión en el shell de vCenter Server e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Seleccione la opción 2, Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados.

3 Escriba el nombre de usuario y la contraseña del administrador.

4 Seleccione Opción 2: Importar certificados personalizados y claves para reemplazar el certificado de firma raíz de VMCA existente y responder a las solicitudes.

   a Especifique la ruta de acceso completa al certificado raíz cuando se le solicite.

   b Si es la primera vez que reemplaza los certificados, se le solicitará información que se utilizará para el certificado SSL de máquina.

   Esta información incluye el FQDN obligatorio de la máquina y se almacena en el archivo `certool.cfg`.

Reemplazar un certificado SSL de máquina por un certificado de VMCA (entidad de certificación intermedia) mediante Certificate Manager

Cuando se utiliza VMCA como entidad de certificación intermedia, se puede reemplazar explícitamente el certificado SSL de máquina mediante la utilidad vSphere Certificate Manager. En primer lugar, reemplace el certificado raíz de VMCA en la instancia de vCenter Server y, a continuación, puede reemplazar el certificado SSL de máquina, que será firmado por la nueva raíz de VMCA. También se puede utilizar esta opción para reemplazar certificados SSL de máquina que se encuentren dañados o a punto de caducar.

Al reemplazar el certificado SSL de máquina existente por un nuevo certificado firmado por VMCA, vSphere Certificate Manager solicita información e introduce todos los valores, excepto la contraseña y la dirección IP de vCenter Server, en el archivo `certool.cfg`.

- Contraseña de administrator@vsphere.local
- Código de país de dos letras
- Nombre de empresa
- Nombre de organización
- Unidad de organización
- Estado
- Localidad
- Dirección IP (opcional)
- Correo electrónico
- Nombre del host, es decir, el nombre de dominio completo de la máquina para la que se desea reemplazar el certificado. Si el nombre del host no coincide con el FQDN, el reemplazo de los certificados no se completa correctamente y el entorno puede quedar en un estado inestable.
- Dirección IP de vCenter Server
- Nombre de VMCA, es decir, el nombre de dominio completo de la máquina en la que se ejecuta la configuración del certificado.

Nota El campo OU (organizationalUnitName) ya no es obligatorio.

Requisitos previos

- Debe conocer la siguiente información para ejecutar vSphere Certificate Manager con esta opción.
  - Contraseña de administrator@vsphere.local.
  - FQDN de la máquina para la cual se desea generar un nuevo certificado firmado por VMCA. Las demás propiedades tienen los valores predeterminados, pero pueden cambiarse.

- Nombre de host o dirección IP del sistema de vCenter Server.

Procedimiento

1 Inicie sesión en el shell de vCenter Server e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Seleccione la opción 3: Reemplazar el certificado SSL de máquina por un certificado de VMCA.

3 Escriba el nombre de usuario y la contraseña del administrador.

4 Responda las solicitudes del sistema.

   vSphere Certificate Manager almacena la información en el archivo `certool.cfg`.

Resultados

vSphere Certificate Manager reemplazará el certificado SSL de máquina.

Reemplazar certificados de usuario de solución por certificados de VMCA (entidad de certificación intermedia) mediante Certificate Manager

Cuando se utiliza VMCA como entidad de certificación intermedia, se puede reemplazar explícitamente el certificado de usuario de solución mediante la utilidad vSphere Certificate Manager. En primer lugar, reemplace el certificado raíz de VMCA en la instancia de vCenter Server y, a continuación, puede reemplazar el certificado de usuario de solución, que será firmado por la nueva raíz de VMCA. También se puede utilizar esta opción para reemplazar certificados de solución que se encuentren dañados o a punto de caducar.

Requisitos previos

- Reinicie todos los nodos de vCenter Server de forma explícita si reemplazó el certificado raíz de VMCA en una implementación que consta de varias instancias de vCenter Server en la configuración de Enhanced Linked Mode.
- Debe conocer la siguiente información para ejecutar vSphere Certificate Manager con esta opción.
  - Contraseña de administrator@vsphere.local
  - Nombre de host o dirección IP del sistema de vCenter Server

Procedimiento

1 Inicie sesión en el shell de vCenter Server e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Seleccione la opción 6: Reemplazar certificados de usuario de solución por certificados de VMCA.

3 Escriba el nombre de usuario y la contraseña del administrador.

4 Responda las solicitudes del sistema.

   Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2112281 para obtener más información.

Resultados

vSphere Certificate Manager reemplazará todos los certificados de usuario de solución.

Reemplazar todos los certificados por certificados personalizados con el Certificate Manager

Es posible usar la utilidad vSphere Certificate Manager para reemplazar todos los certificados por certificados personalizados. Antes de iniciar el proceso, es necesario enviar solicitudes de firma de certificado (CSR) a la entidad de certificación CA. Se puede utilizar Certificate Manager para generar las CSR.

Una opción es reemplazar solo los certificados SSL de máquina y utilizar los certificados de usuario de solución que proporciona VMCA. Los certificados de usuario de solución se utilizan únicamente para la comunicación entre los componentes de vSphere.

Cuando se utilizan certificados personalizados, se deben reemplazar los certificados firmados por VMCA por certificados personalizados. Es posible utilizar vSphere Client, la utilidad vSphere Certificate Manager o las interfaces CLI para reemplazar manualmente los certificados. Los certificados se almacenarán en VECS.

Para reemplazar todos los certificados por certificados personalizados debe ejecutar la utilidad vSphere Certificate Manager varias veces. Los pasos de alto nivel para reemplazar los certificados SSL de máquina y los certificados de usuarios de solución incluyen:

1 Iniciando la utilidad vSphere Certificate Manager.

2 Se generan solicitudes de firma del certificado para el certificado SSL de máquina y los certificados de usuarios de soluciones por separado en cada equipo.

   a Para generar CSR para el certificado SSL de máquina, seleccione la opción 1, Reemplazar el certificado SSL de máquina por un certificado personalizado. Cuando se le solicite de nuevo una opción y seleccione Opción 1: Generar solicitudes de inicio de certificado y claves para el certificado SSL de máquina.

   b Si la directiva de la empresa no permite una implementación híbrida, seleccione la opción 5, Reemplazar certificados de usuarios de solución por certificados personalizados.

3 Envíe la CSR a la CA externa o de la empresa. Recibirá un certificado firmado y un certificado raíz de la CA.

4 Después de recibir los certificados firmados y el certificado raíz de la CA reemplace el certificado SSL de máquina en cada máquina mediante la opción 1 Reemplazar el certificado SSL de máquina por un certificado personalizado.

5 Si también desea reemplazar los certificados de usuario de solución, seleccione la opción 5, Reemplazar certificados de usuario de solución por certificados personalizados.

6 Por último, cuando varias instancias de vCenter Server están conectadas en la configuración de Enhanced Linked Mode, repitiendo el proceso en cada nodo.

Generar solicitudes de firma de certificado con Certificate Manager (certificados personalizados)

Es posible emplear la utilidad vSphere Certificate Manager para generar solicitudes de firma de certificado (Certificate Signing Requests, CSR) y, a continuación, enviarlas a la entidad de certificación empresarial o a una entidad de certificación externa. Los certificados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

Requisitos previos

vSphere Certificate Manager solicita información. La solicitud depende del entorno y del tipo de certificado que se desea reemplazar.

- Para cualquier tipo de generación de CSR, se solicita la contraseña del usuario administrator@vsphere.local o el administrador del dominio de vCenter Single Sign-On con el que se desea establecer la conexión.
- Se le solicita el nombre de host o la dirección IP de vCenter Server.
- Para generar una CSR para un certificado SSL de máquina, se solicitan las propiedades del certificado, que están almacenadas en el archivo `certool.cfg`. En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.

  Nota A partir de vSphere 8.0 y otras versiones posteriores, si utiliza vSphere Certificate Manager para generar la CSR, el tamaño mínimo de la clave pasa de 2048 bits a 3072 bits. En vSphere 8.0 Update 1 y versiones posteriores, utilice vSphere Client para generar una CSR con un tamaño de clave de 2048 bits.

  Nota El certificado FIPS de vSphere solo valida los tamaños de clave RSA de 2048 y 3072 bits.

Procedimiento

1 Inicie sesión en cada instancia de vCenter Server (vCenter Server Shell) de su entorno e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Opción de selección 1, Reemplazar el certificado SSL de máquina por un certificado personalizado.

3 Escriba el nombre de usuario y la contraseña del administrador.

4 Seleccione la opción 1, Generar solicitudes de firma de certificado y claves para el certificado SSL de máquina, si desea generar la CSR, seguir las indicaciones y salir de vSphere Certificate Manager.

   Es necesario especificar un directorio como parte de este proceso. vSphere Certificate Manager colocará los archivos de certificado y de claves en el directorio.

5 Si también desea reemplazar todos los certificados de usuario de la solución, reinicie vSphere Certificate Manager y seleccione la opción 5, Reemplazar los certificados de usuario de solución por certificados personalizados.

6 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de vCenter Server.

7 Seleccione la opción 1, Generar solicitudes de firma de certificado y claves para los certificados de usuario de solución, si desea generar la CSR, seguir las indicaciones y salir de vSphere Certificate Manager.

   Es necesario especificar un directorio como parte de este proceso. Certificate Manager colocará el certificado y los archivos de claves en el directorio.

Pasos siguientes

Para realizar el reemplazo de certificados, consulte Reemplazar un certificado SSL de máquina por un certificado personalizado mediante Certificate Manager.

Reemplazar un certificado SSL de máquina por un certificado personalizado mediante Certificate Manager

Puede usar la utilidad vSphere Certificate Manager para reemplazar el certificado SSL de máquina en cada nodo por un certificado personalizado. El certificado SSL de máquina se utiliza en el servicio de proxy inverso de cada nodo de vCenter Server. Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios.

Requisitos previos

Antes de comenzar, se necesita una CSR para cada máquina del entorno. La CSR se puede generar mediante vSphere Certificate Manager o de forma explícita.

1 Para generar la CSR mediante vSphere Certificate Manager, consulte Generar solicitudes de firma de certificado con Certificate Manager (certificados personalizados).

2 Para generar la CSR de forma explícita, solicite un certificado para cada máquina a la entidad de certificación empresarial o externa. El certificado debe cumplir con los siguientes requisitos:

   - Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
   - Formato CRT
   - x509 versión 3
   - SubjectAltName debe contener DNS Name=<machine_FQDN>.

- Contiene los siguientes usos de claves: firma digital, cifrado de clave

Consulte también el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2112014, Obtener certificados de vSphere de una entidad de certificación de Microsoft.

Procedimiento

1 Inicie sesión en vCenter Server e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Opción de selección 1, Reemplazar el certificado SSL de máquina por un certificado personalizado.

3 Escriba el nombre de usuario y la contraseña del administrador.

4 Seleccione Opción 2: Importar certificados personalizados y claves para reemplazar el certificado SSL de máquina existente para iniciar el reemplazo de certificados y responder a las solicitudes.

   vSphere Certificate Manager solicita la siguiente información:

   - Contraseña de administrator@vsphere.local
   - Un certificado SSL de máquina personalizado y válido (archivo `.crt`)
   - Una clave SSL de máquina personalizada y válida (archivo `.key`)
   - Un certificado de firma válido para el certificado SSL de máquina personalizado (archivo `.crt`)
   - Dirección IP de vCenter Server

Reemplazar certificados de usuario de solución por certificados personalizados mediante el administrador de certificados

Muchas empresas solo requieren que reemplace los certificados de los servicios a los que se puede acceder externamente. Sin embargo, el vSphere Certificate Manager también permite reemplazar certificados de usuarios de solución. Los usuarios de solución son recopilaciones de servicios, por ejemplo, todos los servicios que están asociados a vSphere Client.

Cuando se le solicite un certificado de usuario de solución, proporcione la cadena de certificados de firma completa de la entidad de certificación externa.

El formato debe ser similar al siguiente mensaje.

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
```

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

Requisitos previos

Antes de comenzar, se necesita una CSR para cada máquina del entorno. La CSR se puede generar mediante vSphere Certificate Manager o de forma explícita.

1 Para generar la CSR mediante vSphere Certificate Manager, consulte Generar solicitudes de firma de certificado con Certificate Manager (certificados personalizados).

2 Solicite un certificado para cada usuario de solución en cada nodo a la CA empresarial o externa. Puede generar la CSR mediante vSphere Certificate Manager o prepararla usted mismo. La CSR debe cumplir con los siguientes requisitos:

- Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
- Formato CRT
- x509 versión 3
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Cada certificado de usuario de solución debe tener un `Subject` diferente. Por ejemplo, considere incluir el nombre de usuario de solución (como vpxd) u otro identificador único.
- Contiene los siguientes usos de claves: firma digital, cifrado de clave

Consulte también el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2112014, Obtener certificados de vSphere de una entidad de certificación de Microsoft.

Procedimiento

1 Inicie sesión en vCenter Server e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Seleccione la opción 5. Reemplazar certificados de usuario de solución por certificado personalizado.

3 Escriba el usuario y la contraseña del SSO.

4 Seleccione la opción 2: Importar certificados personalizados y clave(s) para reemplazar los certificados de usuario de solución existentes y responda a las solicitudes.

vSphere Certificate Manager solicita la siguiente información:

- Contraseña de administrator@vsphere.local
- Certificado y clave del usuario de solución de la máquina
- Se le pedirá el certificado y la clave (`vpxd.crt` y `vpxd.key`) para el usuario de solución de la máquina

- Se le pedirá el conjunto completo de certificados y claves (`vpxd.crt` y `vpxd.key`) para todos los usuarios de solución

Revertir la última operación realizada al volver a publicar certificados antiguos mediante el administrador de certificados

Cuando se realiza una operación de administración de certificados mediante la utilidad vSphere Certificate Manager, primero se almacena el estado actual del certificado en BACKUP_STORE, en VECS, antes del reemplazo de los certificados. Es posible revertir la última operación realizada y regresar al estado anterior.

Nota La operación de reversión restablece lo que actualmente se encuentra en BACKUP_STORE. Si ejecuta vSphere Certificate Manager con dos opciones diferentes y, a continuación, intenta hacer la reversión, solo se revierte la última operación.

Procedimiento

1 Inicie sesión en el shell de vCenter Server e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Seleccione la opción 7. Revertir la última operación realizada volviendo a publicar los certificados antiguos.

3 Escriba el nombre de usuario y la contraseña del administrador.

4 Para continuar, introduzca **`Y`**.

Restablecer todos los certificados mediante Certificate Manager

Puede usar la utilidad vSphere Certificate Manager para reemplazar todos los certificados de vCenter existentes por los certificados firmados por VMCA.

Cuando utiliza esta opción, se sobrescriben todos los certificados personalizados que actualmente figuran en VMware Endpoint Certificate Store (VECS).

vSphere Certificate Manager puede reemplazar todos los certificados. Qué certificados se reemplacen dependerá de las opciones que se seleccionen.

Procedimiento

1 Inicie sesión en el shell de vCenter Server e inicie vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Seleccione la opción 8. Restablecer todos los certificados.

3 Escriba el nombre de usuario y la contraseña del administrador.

4 Cuando se le solicite, introduzca la información del certificado.

Pasos siguientes

Una vez que se reemplacen los certificados y se reinicien los servicios, compruebe la información del certificado.

Reemplazar certificados de vSphere de forma manual

En algunos casos especiales de reemplazo de certificados, no se puede usar la utilidad vSphere Certificate Manager. En su lugar, puede usar las CLI incluidas en la instalación para el reemplazo de certificados.

Instrucciones sobre la interrupción y el inicio de servicios de vCenter Server

Para determinadas partes del reemplazo manual de certificados, se deben detener todos los servicios de vCenter Server y, a continuación, iniciar únicamente los servicios que administran la infraestructura de certificados. Al detener los servicios solo cuando es necesario, se reduce el tiempo de inactividad.

Como parte del proceso de reemplazo de certificados, es necesario detener e iniciar los servicios. Puede usar el comando `service-control` para iniciar y detener servicios. Puede iniciar y detener todos los servicios o servicios individuales. Consulte la ayuda de la línea de comandos para obtener más información.

Siga estas directrices.

- No detenga los servicios para generar nuevos pares de claves públicas/privadas o nuevos certificados.
- Si es el único administrador, no es necesario que detenga los servicios al agregar un nuevo certificado raíz. El certificado raíz anterior sigue disponible y todos los servicios pueden seguir autenticándose con ese certificado.
- Detenga los servicios justo antes de eliminar un certificado SSL de máquina en VMware Endpoint Certificate Store (VECS).

Reemplazar los certificados firmado por VMCA existentes por certificados nuevos firmados por VMCA mediante la CLI

Si el certificado raíz de entidad de VMware Certificate Authority (VMCA) está por caducar, o si desea reemplazarlo por otros motivos, puede usar la CLI para generar un certificado raíz nuevo y agregarlo a VMware Directory Service. A continuación, puede generar certificados SSL de máquina y certificados de usuarios de solución nuevos mediante el certificado raíz nuevo.

Use la utilidad vSphere Certificate Manager para reemplazar certificados en la mayoría de los casos.

Si necesita tener un control detallado, este caso ofrece instrucciones detalladas paso a paso para reemplazar el conjunto completo de certificados mediante comandos de CLI. O bien puede reemplazar certificados individuales mediante el procedimiento de la tarea correspondiente.

Requisitos previos

Solo administrator@vsphere.local u otros usuarios del grupo Administradores de CA pueden realizar tareas de administración de certificados. Consulte Agregar miembros a un grupo de vCenter Single Sign-On.

Generar un nuevo certificado raíz firmado por VMCA mediante la CLI

Puede generar nuevos certificados firmados por VMCA con la CLI `certool` y publicar los certificados en vmdir.

Procedimiento

1 En vCenter Server, genere un nuevo certificado autofirmado y una clave privada.

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

2 Reemplace el certificado raíz existente con el nuevo certificado.

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

El comando genera el certificado, lo agrega a vmdir y, a continuación, lo agrega a VECS.

3 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 (opcional) Publique el nuevo certificado raíz en vmdir.

```
dir-cli trustedcert publish --cert newRoot.crt
```

El comando actualiza todas las instancias de vmdir de manera inmediata. Si no lo ejecuta, la propagación del nuevo certificado a todos los nodos puede tardar un poco.

5 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Generar un nuevo certificado raíz firmado por VMCA

El siguiente ejemplo muestra todos los pasos para comprobar la información de la entidad de certificación raíz actual y volver a generar el certificado raíz.

1 (Opcional) En vCenter Server, enumere el certificado raíz de VMCA para asegurarse de que se encuentre en el almacén de certificados.

```
/usr/lib/vmware-vmca/bin/certool --getrootca
```

La salida tiene un aspecto similar al siguiente:

```
output:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
    ...
```

2 (Opcional) Enumere el almacén TRUSTED_ROOTS de VECS y compare el número de serie del certificado con la salida del paso 1.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry list --store TRUSTED_ROOTS --text
```

En el caso más simple con un solo certificado raíz, la salida tiene un aspecto similar al siguiente:

```
Number of entries in store :    1
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :    Trusted Cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
```

3 Genere un nuevo certificado raíz de VMCA. El comando agrega el certificado al almacén TRUSTED_ROOTS en VECS y en vmdir (VMware Directory Service).

```
/usr/lib/vmware-vmca/bin/certool --selfca --config=/usr/lib/vmware-vmca/share/config/
certool.cfg
```

Reemplazar los certificados SSL de máquina por certificados firmados por VMCA mediante la CLI

Después de generar un nuevo certificado raíz firmado por VMCA, puede usar el comando `vecs-cli`para reemplazar todos los certificados SSL de máquina en el entorno.

Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. Cuando varias instancias de vCenter Server están conectadas en la configuración de Enhanced Linked Mode, debe ejecutar los comandos de generación de certificados SSL de máquina en cada nodo.

Requisitos previos

Prepárese para detener todos los servicios y para iniciar los servicios que controlan la propagación y el almacenamiento de certificados.

Procedimiento

1 Haga una copia de `certool.cfg` para cada máquina que necesite un certificado nuevo.

   Puede encontrar el archivo `certool.cfg` en el directorio `/usr/lib/vmware-vmca/share/config/`.

2 Edite el archivo de configuración personalizado de cada máquina a fin de incluir el FQDN de la máquina.

   Ejecute `NSLookup` sobre la dirección IP de la máquina a fin de ver el listado de DNS del nombre y usar ese nombre en el campo Nombre de host del archivo.

3 Genere un par de archivos de clave pública/privada y un certificado para cada archivo pasando el archivo de configuración que acaba de personalizar.

   Por ejemplo:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Agregue el certificado nuevo a VECS.

   Todas las máquinas necesitan el certificado nuevo en el almacén de certificados local para comunicarse mediante SSL. Primero debe eliminar la entrada existente y, a continuación, agregar la nueva.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.crt
--key machine1.priv
```

6 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Reemplazo de certificados de una máquina por certificados firmados por VMCA

1 Cree un archivo de configuración para el certificado SSL y guárdelo como `ssl-config.cfg` en el directorio actual.

```
Country = US
Name = vmca-<FQDN-example>
Organization = <my_company>
```

```
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

2 Genere un par de claves para el certificado SSL de máquina. En una implementación de varias instancias de vCenter Server conectadas en la configuración de Enhanced Linked Mode, ejecute este comando en cada nodo de vCenter Server.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=ssl-key.priv --pubkey=ssl-key.pub
```

Los archivos `ssl-key.priv` y `ssl-key.pub` se crean en el directorio actual.

3 Genere el nuevo certificado SSL de máquina. Este certificado está firmado por VMCA. Si reemplazó el certificado raíz de VMCA por un certificado personalizado, VMCA firma todos los certificados con la cadena completa.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

El archivo `new-vmca-ssl.crt` se crea en el directorio actual.

4 (Opcional) Enumere el contenido de VECS.

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- Ejemplo de salida en vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

5 Reemplace el certificado SSL de máquina en VECS por el nuevo certificado SSL de máquina. Los valores `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados.

- En cada instancia de vCenter Server, ejecute los siguientes comandos para actualizar el certificado SSL de máquina en el almacén MACHINE_SSL_CERT. Debe actualizar el certificado para cada máquina por separado, ya que cada una de ellas tiene un FQDN diferente.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
__MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Pasos siguientes

También puede reemplazar los certificados de sus hosts ESXi. Consulte la publicación *Seguridad de vSphere*.

Reemplazar los certificados de usuarios de solución por certificados nuevos firmados por VMCA mediante la CLI

Después de reemplazar los certificados SSL de máquina, puede utilizar el comando `dir-cli` para reemplazar todos los certificados de usuarios de solución. Los certificados de usuario de solución deben ser válidos, es decir, que no estén caducados, pero la infraestructura de certificados no utiliza ninguna otra información del certificado.

Muchos clientes de VMware no reemplazan los certificados de usuario de las soluciones. Reemplazan solo los certificados SSL de los equipos con certificados personalizados. Este enfoque híbrido satisface los requisitos de sus equipos de seguridad.

- Los certificados se sientan detrás de un proxy, o bien son certificados personalizados.
- No se utilizan CA intermedias.

Se reemplaza el certificado de usuario de solución de la máquina y el certificado de usuario de solución en cada sistema vCenter Server.

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `/usr/lib/vmware-vmafd/bin/dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

Requisitos previos

Prepárese para detener todos los servicios y para iniciar los servicios que controlan la propagación y el almacenamiento de certificados.

Procedimiento

1 Haga una copia de `certool.cfg`, quite los campos Nombre, Dirección IP, Correo electrónico y Nombre DNS, y cambie el nombre del archivo: por ejemplo, a `sol_usr.cfg`.

   Se pueden nombrar los certificados desde la línea de comandos como parte de la generación. La otra información no es necesaria para los usuarios de solución. Si se deja la información predeterminada, los certificados generados podrían resultar confusos.

2 Genere un par de archivos de clave pública/privada y un certificado para cada usuario de solución y pase el archivo de configuración que recién personalizó.

   Por ejemplo:

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
/usr/lib/vmware-vmca/bin/certool --gencert --privkey=vpxd.priv --cert vpxd.crt --
Name=VPXD_1 --config sol_usr.cfg
```

3 Busque el nombre de cada usuario de solución.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
```

   Puede usar el identificador único que se devuelve al reemplazar los certificados. La entrada y la salida deben verse de la siguiente manera.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

   En una implementación de varias instancias de vCenter Server conectadas en la configuración de Enhanced Linked Mode, el resultado de `/usr/lib/vmware-vmafd/bin/dir-cli service list` incluye todos los usuarios de solución de todos los nodos. Ejecute `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 En cada usuario de solución, reemplace el certificado actual en vmdir y, a continuación, en VECS.

El siguiente ejemplo muestra cómo reemplazar los certificados del servicio vpxd.

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --
cert ./vpxd.crt
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt
--key vpxd.priv
```

Nota Los usuarios de solución no podrán autenticarse en vCenter Single Sign-On si no se reemplaza el certificado en vmdir.

6 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Usar los certificados de usuarios de solución firmados por VMCA

1 Genere un par de claves pública/privada para cada usuario de solución en cada nodo de vCenter Server en una configuración de Enhanced Linked Mode. Esto incluye un par para la solución de máquina y un par para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient, wcp).

a Genere un par de claves para el usuario de solución de la máquina.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-
key.pub
```

b Genere un par de claves para el usuario de solución vpxd en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c Genere un par de claves para el usuario de solución vpxd-extension en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --
pubkey=vpxd-extension-key.pub
```

d Genere un par de claves para el usuario de solución vsphere-webclient en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --
pubkey=vsphere-webclient-key.pub
```

e Genere un par de claves para el usuario de solución wcp en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 Genere certificados de usuario de solución que estén firmados con el nuevo certificado raíz de VMCA para el usuario de solución de la máquina y para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient, wcp) en cada nodo de vCenter Server.

Nota El parámetro `--Name` tiene que ser único. Al incluir el nombre del almacén del usuario de solución, resulta más fácil ver qué certificado se asigna a cada usuario de solución. El ejemplo incluye el nombre, por ejemplo, `vpxd` o `vpxd-extension` en cada caso.

a Haga una copia del archivo `/usr/lib/vmware-vmca/share/config/certool.cfg` y, a continuación, modifique o elimine los campos Nombre, Dirección IP, Nombre de DNS y Correo electrónico según sea necesario, y cambie el nombre del archivo (por ejemplo, a `sol_usr.cfg`).

b Genere un certificado para el usuario de solución de la máquina en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine --config sol_usr.cfg
```

c Genere un certificado para el usuario de solución vpxd en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv
--Name=vpxd --config sol_usr.cfg
```

d Genere un certificado para el usuario de solución vpxd-extensions en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension --config sol_usr.cfg
```

e Ejecute el siguiente comando para generar un certificado para el usuario de solución vsphere-webclient en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --config sol_usr.cfg
```

f Ejecute el siguiente comando para generar un certificado para el usuario de solución wcp en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp --config sol_usr.cfg
```

3 Reemplace los certificados de usuario de solución en VECS por los nuevos certificados de usuario de solución.

Nota Los parámetros `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados de los servicios.

---

a Reemplace el certificado de usuario de solución de la máquina en cada nodo:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine.crt --key machine-key.priv
```

b Reemplace el certificado de usuario de solución vpxd en cada nodo.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c Reemplace el certificado de usuario de solución vpxd-extension en cada nodo.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e Reemplace el certificado de usuario de solución wcp en cada nodo.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-key.priv
```

4 Actualice VMware Directory Service (vmdir) con los nuevos certificados de usuarios de solución. Se solicita una contraseña de administrador de vCenter Single Sign-On.

a Ejecute `/usr/lib/vmware-vmafd/bin/dir-cli service list` para obtener el sufijo de identificador único de servicio para cada usuario de solución. Este comando se ejecuta en un sistema vCenter Server.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
```

```
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `/usr/lib/vmware-vmafd/bin/dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

b Reemplace el certificado de máquina en vmdir en cada nodo de vCenter Server. Por ejemplo, si machine-6fd7f140-60a9-11e4-9e28-005056895a69 es el usuario de solución de la máquina en vCenter Server, ejecute el siguiente comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
```

c Reemplace el certificado de usuario de solución vpxd en vmdir en cada nodo. Por ejemplo, si vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd, ejecute el siguiente comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d Reemplace el certificado de usuario de solución vpxd-extension en vmdir en cada nodo. Por ejemplo, si vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd-extension, ejecute el siguiente comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo. Por ejemplo, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vsphere-webclient, ejecute el siguiente comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f Reemplace el certificado de usuario de solución wcp en cada nodo. Por ejemplo, si wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e es el ID del usuario de solución wcp, ejecute este comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

Pasos siguientes

Reinicie todos los servicios en cada nodo de vCenter Server.

Convertir VMCA en una entidad de certificación intermedia mediante la CLI

Puede usar la CLI para reemplazar el certificado raíz de VMCA por un certificado externo firmado por una entidad de certificación en la que se incluya VMCA en la cadena de certificados. Más adelante, todos los certificados generados por VMCA incluirán la cadena completa. Puede reemplazar los certificados existentes por certificados generados recientemente.

Si utiliza VMCA como una entidad de certificación intermedia o utiliza certificados personalizados, es posible que experimente una complejidad considerable y que exista la posibilidad de un impacto negativo para la seguridad, así como un aumento innecesario en el riesgo operativo. Para obtener más información sobre la administración de certificados en un entorno de vSphere, consulte la publicación de blog llamada *Revisión de producto nuevo: reemplazo del certificado SSL de vSphere híbrido* en http://vmware.com/go/hybridvmca.

Reemplazar el certificado raíz (entidad de certificación intermedia) mediante la CLI

El primer paso para reemplazar los certificados VMCA por certificados personalizados es generar una CSR y enviarla para su firma. A continuación, use la CLI para agregar el certificado firmado a VMCA como certificado raíz.

Se puede utilizar la utilidad Certificate Manager u otra herramienta para generar la CSR. La CSR debe cumplir con los siguientes requisitos:

- Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
- x509 versión 3
- Para certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos. Por ejemplo:

  ```
  basicConstraints        = critical,CA:true
  keyUsage                = critical,digitalSignature,keyCertSign
  ```

- La firma CRL debe estar habilitada.
- Uso mejorado de clave puede estar vacío o contener autenticación del servidor.
- No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados.
- No se admiten los certificados con comodines o con más de un nombre DNS.
- No se pueden crear CA subsidiarias de VMCA.

Para obtener un ejemplo de uso de la entidad de certificación de Microsoft, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2112009, Crear una plantilla de entidad de certificación de Microsoft para creación de certificados SSL en vSphere 6.x.

Nota El certificado FIPS de vSphere solo valida los tamaños de clave RSA de 2048 y 3072 bits.

VMCA valida los siguientes atributos de certificados al reemplazar el certificado raíz:

- Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo).
- Uso de clave: firma de certificado
- Restricción básica: entidad de certificación de tipo sujeto

Procedimiento

1 Genere una CSR y envíela a la entidad de certificación.

  Siga las instrucciones de la entidad de certificación.

2 Prepare un archivo de certificado que incluya el certificado VMCA firmado y la cadena de entidad de certificación completa de la entidad de certificación empresarial o de terceros. Guarde el archivo, por ejemplo como `rootca1.crt`.

  Para aplicar este paso, se pueden copiar todos los certificados de la entidad de certificación en formato PEM en un solo archivo. Comience con el certificado raíz VMCA y termine con el certificado raíz PEM de la entidad de certificación. Por ejemplo:

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 Reemplace la entidad de certificación raíz VMCA existente.

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

Al ejecutarse, este comando realiza lo siguiente:

- Agrega el nuevo certificado raíz personalizado a la ubicación de certificados en el sistema de archivos.
- Anexa el certificado raíz personalizado al almacén TRUSTED_ROOTS en VECS (después de una demora).
- Agrega el certificado raíz personalizado a vmdir (después de una demora).

5 (opcional) Para propagar el cambio a todas las instancias de vmdir (VMware Directory Service), publique el nuevo certificado raíz en vmdir suministrando la ruta de acceso para cada archivo.

Por ejemplo, si el certificado solo tiene un certificado en la cadena:

```
dir-cli trustedcert publish --cert rootca1.crt
```

Si el certificado tiene más de un certificado en la cadena:

```
dir-cli trustedcert publish --cert rootcal.crt --chain
```

Cada 30 segundos se produce la replicación entre los nodos de vmdir. No se necesita agregar el certificado raíz a VECS explícitamente, ya que VECS sondea vmdir cada 5 minutos en busca de nuevos archivos de certificados raíz.

6 (opcional) Si fuera necesario, se puede forzar la actualización de VECS.

```
vecs-cli force-refresh
```

7 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Reemplazo del certificado raíz

Reemplace el certificado raíz de VMCA por el certificado raíz personalizado de la entidad de certificación mediante el comando `certool` con la opción `--rootca`.

```
/usr/lib/vmware-vmca/bin/certool --rootca --cert=<path>/root.pem --privkey=<path>/root.key
```

Al ejecutarse, este comando realiza lo siguiente:

- Agrega el nuevo certificado raíz personalizado a la ubicación de certificados en el sistema de archivos.
- Anexa el certificado raíz personalizado al almacén TRUSTED_ROOTS en VECS.
- Agrega el certificado raíz personalizado a vmdir.

Pasos siguientes

Se puede eliminar el certificado raíz original de VMCA del almacén de certificados si así lo establece la directiva de la empresa. Si se hace eso, es necesario reemplazar el certificado de firma de vCenter Single Sign-On. Consulte Reemplazar un certificado vCenter Server STS mediante la línea de comandos.

Reemplazar certificados SSL de máquina (entidad de certificación intermedia) mediante la CLI

Después de recibir el certificado firmado de la CA puede usar la CLI para convertirlo en el certificado raíz de VMCA y reemplazar todos los certificados SSL de máquina.

Estos pasos son prácticamente los mismos que los pasos para reemplazar un certificado por otro que utilice VMCA como entidad de certificación. Sin embargo, en este caso, VMCA firma todos los certificados con la cadena completa.

Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. Cuando varias instancias de vCenter Server están conectadas en la configuración de Enhanced Linked Mode, debe ejecutar los comandos de generación de certificados SSL de máquina en cada nodo.

Requisitos previos

Para el certificado SSL de máquina, el `SubjectAltName` debe contener `DNS Name=<Machine FQDN>`.

Procedimiento

1 Haga una copia de `certool.cfg` para cada máquina que necesite un certificado nuevo.

   El archivo `certool.cfg`, se encuentra en el directorio `/usr/lib/vmware-vmca/share/config/`.

2 Edite el archivo de configuración personalizado de cada máquina a fin de incluir el FQDN de la máquina.

   Ejecute `NSLookup` sobre la dirección IP de la máquina a fin de ver el listado de DNS del nombre y usar ese nombre en el campo Nombre de host del archivo.

3 Genere un par de archivos de clave pública/privada y un certificado para cada máquina pasando el archivo de configuración que acaba de personalizar.

   Por ejemplo:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Agregue el certificado nuevo a VECS.

Todas las máquinas necesitan el certificado nuevo en el almacén de certificados local para comunicarse mediante SSL. Primero debe eliminar la entrada existente y, a continuación, agregar la nueva.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Reemplazo de certificados SSL de máquina (VMCA es la CA intermedia)

1 Cree un archivo de configuración para el certificado SSL y guárdelo como `ssl-config.cfg` en el directorio actual.

```
Country = US
Name = vmca-<FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 Genere un par de claves para el certificado SSL de máquina. En una implementación de varias instancias de vCenter Server conectadas en la configuración de Enhanced Linked Mode, ejecute este comando en cada nodo de vCenter Server.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=ssl-key.priv --pubkey=ssl-key.pub
```

Los archivos `ssl-key.priv` y `ssl-key.pub` se crean en el directorio actual.

3 Genere el nuevo certificado SSL de máquina. Este certificado está firmado por VMCA. Si reemplazó el certificado raíz de VMCA por un certificado personalizado, VMCA firma todos los certificados con la cadena completa.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

El archivo `new-vmca-ssl.crt` se crea en el directorio actual.

4 (Opcional) Enumere el contenido de VECS.

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- Ejemplo de salida en vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

5 Reemplace el certificado SSL de máquina en VECS por el nuevo certificado SSL de máquina. Los valores `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados.

- En cada instancia de vCenter Server, ejecute los siguientes comandos para actualizar el certificado SSL de máquina en el almacén MACHINE_SSL_CERT. Debe actualizar el certificado para cada máquina por separado, ya que cada una de ellas tiene un FQDN diferente.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
__MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Reemplazar certificados de usuario de solución (entidad de certificación intermedia) mediante la CLI

Después de reemplazar los certificados SSL de máquina, puede usar el CLI para reemplazar los certificados de usuarios de solución.

Muchos clientes de VMware no reemplazan los certificados de usuario de las soluciones. Reemplazan solo los certificados SSL de los equipos con certificados personalizados. Este enfoque híbrido satisface los requisitos de sus equipos de seguridad.

- Los certificados se sientan detrás de un proxy, o bien son certificados personalizados.
- No se utilizan CA intermedias.

Se reemplaza el certificado de usuario de solución de la máquina y el certificado de usuario de solución en cada sistema vCenter Server.

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `/usr/lib/vmware-vmafd/bin/dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

Requisitos previos

Cada certificado de usuario de solución debe tener un `Subject` diferente. Por ejemplo, considere incluir el nombre de usuario de solución (como vpxd) u otro identificador único.

Procedimiento

1 Haga una copia de `certool.cfg`, quite los campos Nombre, Dirección IP, Correo electrónico y Nombre DNS, y cambie el nombre del archivo: por ejemplo, a `sol_usr.cfg`.

   Se pueden nombrar los certificados desde la línea de comandos como parte de la generación. La otra información no es necesaria para los usuarios de solución. Si se deja la información predeterminada, los certificados generados podrían resultar confusos.

2 Genere un par de archivos de clave pública/privada y un certificado para cada usuario de solución y pase el archivo de configuración que recién personalizó.

   Por ejemplo:

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 Busque el nombre de cada usuario de solución.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
```

   Puede usar el identificador único que se devuelve al reemplazar los certificados. La entrada y la salida deben verse de la siguiente manera.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

   En una implementación de varias instancias de vCenter Server conectadas en la configuración de Enhanced Linked Mode, el resultado de `/usr/lib/vmware-vmafd/bin/`

`dir-cli service list` incluye todos los usuarios de solución de todos los nodos. Ejecute `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Reemplace el certificado que ya existe primero en vmdir y después en VECS.

Debe agregar los certificados en ese orden para los usuarios de solución. Por ejemplo:

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

Nota Los usuarios de solución no pueden iniciar sesión en vCenter Single Sign-On si no reemplaza el certificado en vmdir.

6 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Reemplazo de certificados de usuarios de solución (entidad de certificación intermedia)

1 Genere un par de claves pública/privada para cada usuario de solución en cada nodo de vCenter Server en una configuración de Enhanced Linked Mode. Esto incluye un par para la solución de máquina y un par para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient, wcp).

a Genere un par de claves para el usuario de solución de la máquina.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-
key.pub
```

b Genere un par de claves para el usuario de solución vpxd en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c Genere un par de claves para el usuario de solución vpxd-extension en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --
pubkey=vpxd-extension-key.pub
```

d Genere un par de claves para el usuario de solución vsphere-webclient en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --
pubkey=vsphere-webclient-key.pub
```

e Genere un par de claves para el usuario de solución wcp en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 Genere certificados de usuario de solución que estén firmados con el nuevo certificado raíz de VMCA para el usuario de solución de la máquina y para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient, wcp) en cada nodo de vCenter Server.

Nota El parámetro `--Name` tiene que ser único. Al incluir el nombre del almacén del usuario de solución, resulta más fácil ver qué certificado se asigna a cada usuario de solución. El ejemplo incluye el nombre, por ejemplo, `vpxd` o `vpxd-extension` en cada caso.

a Haga una copia del archivo `/usr/lib/vmware-vmca/share/config/certool.cfg` y, a continuación, modifique o elimine los campos Nombre, Dirección IP, Nombre de DNS y Correo electrónico según sea necesario, y cambie el nombre del archivo (por ejemplo, a `sol_usr.cfg`).

b Genere un certificado para el usuario de solución de la máquina en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine --config sol_usr.cfg
```

c Genere un certificado para el usuario de solución vpxd en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv
--Name=vpxd --config sol_usr.cfg
```

d Genere un certificado para el usuario de solución vpxd-extensions en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension --config sol_usr.cfg
```

e Ejecute el siguiente comando para generar un certificado para el usuario de solución vsphere-webclient en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --config sol_usr.cfg
```

f Ejecute el siguiente comando para generar un certificado para el usuario de solución wcp en cada nodo.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp --config sol_usr.cfg
```

3 Reemplace los certificados de usuario de solución en VECS por los nuevos certificados de usuario de solución.

Nota Los parámetros `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados de los servicios.

a Reemplace el certificado de usuario de solución de la máquina en cada nodo:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine.crt --key machine-key.priv
```

b Reemplace el certificado de usuario de solución vpxd en cada nodo.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c Reemplace el certificado de usuario de solución vpxd-extension en cada nodo.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e Reemplace el certificado de usuario de solución wcp en cada nodo.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-key.priv
```

4 Actualice VMware Directory Service (vmdir) con los nuevos certificados de usuarios de solución. Se solicita una contraseña de administrador de vCenter Single Sign-On.

a Ejecute `/usr/lib/vmware-vmafd/bin/dir-cli service list` para obtener el sufijo de identificador único de servicio para cada usuario de solución. Este comando se ejecuta en un sistema vCenter Server.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
```

```
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `/usr/lib/vmware-vmafd/bin/dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

b Reemplace el certificado de máquina en vmdir en cada nodo de vCenter Server. Por ejemplo, si machine-6fd7f140-60a9-11e4-9e28-005056895a69 es el usuario de solución de la máquina en vCenter Server, ejecute el siguiente comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
```

c Reemplace el certificado de usuario de solución vpxd en vmdir en cada nodo. Por ejemplo, si vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd, ejecute el siguiente comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d Reemplace el certificado de usuario de solución vpxd-extension en vmdir en cada nodo. Por ejemplo, si vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd-extension, ejecute el siguiente comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo. Por ejemplo, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vsphere-webclient, ejecute el siguiente comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f Reemplace el certificado de usuario de solución wcp en cada nodo. Por ejemplo, si wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e es el ID del usuario de solución wcp, ejecute este comando:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

Reemplazar certificados por certificados personalizados mediante la CLI

Si la directiva de la empresa lo requiere, puede usar la CLI para reemplazar todos o algunos de los certificados utilizados en vSphere por certificados firmados por una CA de la empresa o externa. Si lo hace, VMCA no estará en la cadena de certificados. Es su responsabilidad almacenar todos los certificados de vCenter en VECS.

Puede reemplazar todos los certificados o utilizar una solución híbrida. Por ejemplo, considere reemplazar todos los certificados que se utilizan para el tráfico de red y dejar los certificados de usuarios de solución firmados por VMCA. Los certificados de usuarios de solución se utilizan solo para efectuar la autenticación en vCenter Single Sign-On. vCenter Server utiliza certificados de usuarios de solución solo para la comunicación interna. Los certificados de usuarios de solución no se utilizan para la comunicación externa.

Nota Si no desea utilizar VMCA, es su responsabilidad reemplazar todos los certificados, aprovisionar componentes nuevos con certificados y hacer un seguimiento de la caducidad de los certificados.

Incluso si decide utilizar certificados personalizados, puede continuar usando la utilidad de VMware Certificate Manager para reemplazar los certificados. Consulte Reemplazar todos los certificados por certificados personalizados con el Certificate Manager.

Si tiene problemas con vSphere Auto Deploy después de reemplazar los certificados, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2000988.

Solicitar certificados e importar un certificado raíz personalizado mediante la CLI

Puede utilizar certificados personalizados de una CA de la empresa o externa. El primer paso es solicitar los certificados a la entidad de certificación y luego usar la CLI para importar los certificados raíz en VMware Endpoint Certificate Store (VECS).

Requisitos previos

El certificado debe cumplir con los siguientes requisitos:

- Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
- x509 versión 3
- Para los certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos.
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Formato CRT
- Contiene los siguientes usos de claves: firma digital, cifrado de clave
- Hora de inicio de un día anterior a la hora actual.

- CN (y SubjectAltName) establecidos con el nombre de host (o dirección IP) que el host ESXi tiene en el inventario de vCenter Server.

Nota El certificado FIPS de vSphere solo valida los tamaños de clave RSA de 2048 y 3072 bits.

Procedimiento

1 Envíe las solicitudes de firma de certificados (Certificate Signing Requests, CSR) para los siguientes certificados al proveedor de certificados de la empresa o externo.

   - Un certificado SSL de máquina para cada máquina. Para el certificado SSL de máquina, el campo SubjectAltName debe contener el nombre de dominio completo (DNS NAME=*FQDN_de_máquina*).
   - Opcionalmente, cinco certificados de usuario de solución para cada nodo. Los certificados de usuario de solución no necesitan incluir la dirección IP, el nombre del host ni la dirección de correo electrónico. Cada certificado debe tener un asunto de certificado diferente.

   Generalmente, el resultado es un archivo PEM para la cadena de confianza, junto con los certificados SSL firmados para cada nodo de vCenter Server.

2 Enumere los almacenes TRUSTED_ROOTS y SSL de máquina.

```
vecs-cli store list
```

   a Asegúrese de que el certificado raíz actual y todos los certificados SSL de máquina estén firmados por VMCA.

   b Anote el contenido de los campos Número de serie, Emisor y Nombre común de asunto.

   c (opcional) Con un explorador web, abra una conexión HTTPS al nodo en el que se reubicará el certificado, mire la información del certificado y asegúrese de que esta coincida con la del certificado SSL de máquina.

3 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 Publique el certificado raíz personalizado.

```
dir-cli trustedcert publish --cert <my_custom_root>
```

   Si no especifica un nombre de usuario y una contraseña en la línea de comandos, el sistema se lo solicitará.

5 Reinicie todos los servicios.

```
service-control --start --all
```

Pasos siguientes

Se puede eliminar el certificado raíz original de VMCA del almacén de certificados si así lo establece la directiva de la empresa. Si se hace eso, es necesario actualizar el certificado de vCenter Single Sign-On. Consulte Reemplazar un certificado vCenter Server STS mediante la línea de comandos.

Reemplazar certificados SSL de máquina por certificados personalizados mediante la CLI

Después de recibir los certificados personalizados, puede usar la CLI para reemplazar los certificados de cada máquina.

Para poder empezar a reemplazar los certificados, debe tener la siguiente información:

- Contraseña de administrator@vsphere.local
- Un certificado SSL de máquina personalizado y válido (archivo `.crt`)
- Una clave SSL de máquina personalizada y válida (archivo `.key`)
- Un certificado personalizado válido para la raíz (archivo `.crt`)

Requisitos previos

Seguramente recibió un certificado para cada máquina de la CA de la empresa o externa.

- Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
- Formato CRT
- x509 versión 3
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Contiene los siguientes usos de claves: firma digital, cifrado de clave

Realice los pasos en cada host de vCenter Server.

Procedimiento

1 Realice una copia de seguridad del certificado SSL de máquina actual.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias
__MACHINE_CERT > oldmachine.crt
/usr/lib/vmware-vmafd/bin/vecs-cli entry getkey --store MACHINE_SSL_CERT --alias
__MACHINE_CERT > oldmachinekey.key
```

2 Inicie sesión en cada host y agregue los nuevos certificados de máquina que reciba de la entidad de certificación a VECS.

   Todos los hosts necesitan el certificado nuevo en el almacén de certificados local para comunicarse mediante SSL.

   a Elimine el certificado existente.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
   __MACHINE_CERT
   ```

   b Agregue el nuevo certificado.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
   __MACHINE_CERT --cert <cert-file-path> --key <key-file-path>
   ```

3 Extraiga el hash del certificado antiguo que se va a reemplazar.

   ```
   openssl x509 -in <path_to_old_machinessl_certificate> -noout -sha1 -fingerprint
   ```

   Aparece un resultado similar al siguiente:

   ```
   SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88
   ```

4 Actualice el endpoint de registro del servicio de búsqueda manualmente.

   ```
   /usr/lib/vmware-lookupsvc/tools/ls_update_certs.py --url https://<vCenterServer_FQDN>/
   lookupservice/sdk --certfile <cert-file-path> --user 'administrator@vsphere.local' --
   password '<password>' --fingerprint <SHA1_hash_of_the_old_certificate_to_replace>
   ```

   Si tiene problemas al ejecutar `ls_update_certs.py`, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/95982.

5 Reinicie todos los servicios.

   ```
   service-control --stop --all && service-control --start --all
   ```

Referencia de comandos de CLI de servicios y certificados de vSphere

3

Puede administrar los certificados VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store), VMware Directory Service (vmdir) y del servicio de token de seguridad (STS) mediante un conjunto de CLI. La utilidad vSphere Certificate Manager también admite muchas tareas relacionadas, pero las CLI son necesarias para la administración manual de certificados y para administrar otros servicios.

Normalmente, las herramientas de CLI se usan para administrar los certificados y los servicios asociados mediante SSH con el fin de conectarse al shell del dispositivo. Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2100508 para obtener más información.

Reemplazar certificados de vSphere de forma manual proporciona ejemplos de reemplazo de certificados mediante comandos de CLI.

Tabla 3-1. vSphere CLI Tools para administrar certificados y servicios asociados

CLI	Descripción	Consulte
`certool`	Genere y administre certificados y claves. Parte de VMCAD, el servicio VMware Certificate Management.	Referencia de comandos de inicialización de certool
`vecs-cli`	Administre el contenido de las instancias de VMware Certificate Store. Parte de VMware Authentication Framework Daemon (VMAFD).	Referencia de comandos vecs-cli
`dir-cli`	Cree y actualice los certificados en VMware Directory Service. Parte de VMAFD.	Referencia de comando dir-cli
`sso-config.sh`	Administre certificados de STS.	Ayuda de línea de comandos. Al introducir `sso-config.sh` sin opciones, se muestra la ayuda de la línea de comandos.
`service-control`	Inicie o detenga los servicios (por ejemplo, como parte de un flujo de trabajo de reemplazo de certificados).	Ejecute este comando para detener los servicios antes de ejecutar otros comandos de la CLI.

Ubicaciones de la CLI de vSphere

De forma predeterminada, las CLI se encuentran en las siguientes ubicaciones.

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

Nota El comando `service-control` no requiere que especifique la ruta de acceso.

Privilegios necesarios para ejecutar las CLI de vSphere

Los privilegios necesarios dependen de la CLI que esté usando y del comando que quiera ejecutar. Por ejemplo, para la mayoría de las operaciones de administración de certificados, tiene que ser administrador para el dominio de vCenter Single Sign-On local (vsphere.local de manera predeterminada). Algunos comandos están disponibles para todos los usuarios.

dir-cli

Debe ser miembro de un grupo de administradores en el dominio local (vsphere.local de manera predeterminada) para ejecutar los comandos `dir-cli`. Si no especifica un nombre de usuario y una contraseña, se le pedirá la contraseña para el administrador del dominio de vCenter Single Sign-On local, administrator@vsphere.local de manera predeterminada.

vecs-cli

Inicialmente, solo el propietario del almacén y los usuarios con privilegios de acceso ilimitado tienen acceso a un almacén. Los usuarios del grupo Administradores tienen privilegios de acceso global.

Los almacenes MACHINE_SSL_CERT y TRUSTED_ROOTS son almacenes especiales. Solo el usuario raíz o el usuario administrador, según el tipo de instalación, tienen acceso total.

certool

La mayoría de los comandos `certool` requieren que el usuario esté en el grupo de administradores. Todos los usuarios pueden ejecutar los siguientes comandos.

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`

- `viewcert`

Cambiar las opciones de configuración de certool

Al ejecutar `certool --gencert` u otros comandos específicos de inicialización o administración de certificados, el comando lee todos los valores de un archivo de configuración. Puede editar el archivo existente, anular el archivo de configuración predeterminado con la opción `--config=<file name>` o anular los diferentes valores en la línea de comandos.

El archivo de configuración, `certool.cfg`, se encuentra en el directorio `/usr/lib/vmware-vmca/share/config/` de forma predeterminada.

El archivo tiene varios campos con los siguientes valores predeterminados:

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

Nota El campo OU (organizationalUnitName) ya no es obligatorio.

Puede cambiar los valores especificando un archivo modificado en la línea de comandos o anulando valores individuales en la línea de comandos, de la siguiente manera.

- Cree una copia del archivo de configuración y edite el archivo. Use la opción de línea de comandos `--config` para especificar el archivo. Especifique la ruta completa para evitar problemas con el nombre de la ruta.
- ```
  /usr/lib/vmware-vmca/bin/certool --gencert --config /tmp/myconfig.cfg
  ```
- Anule los valores individuales en la línea de comandos. Por ejemplo, para anular la localidad, ejecute el siguiente comando:

  ```
  /usr/lib/vmware-vmca/bin/certool --gencert --privkey=private.key --Locality="Mountain
  View"
  ```

Especifique `--Name` para reemplazar el campo Nombre común del nombre de asunto del certificado.

- Para los certificados de usuarios de solución, el nombre es <sol_user name>@<domain> por convención, pero puede cambiarlo si se utiliza una convención diferente en el entorno.
- Para los certificados SSL de máquina, se utiliza el FQDN de la máquina.
  ```

VMCA permite solo un DNSName (en el campo `Hostname`) y ninguna otra opción de alias. Si es el usuario quien especifica la dirección IP, esta también se almacena en SubAltName.

Use el parámetro `--Hostname` para especificar el DNSName de SubAltName del certificado.

Lea los siguientes temas a continuación:

- Referencia de comandos de inicialización de certool
- Referencia de comandos de administración de certool
- Referencia de comandos vecs-cli
- Referencia de comando dir-cli

Referencia de comandos de inicialización de certool

Los comandos de inicialización de `certool` permiten generar solicitudes de firma de certificados, ver y generar certificados y claves firmadas por VMware Certificate Authority (VMCA), importar certificados raíz y realizar otras operaciones de administración de certificados.

En muchos casos, se puede pasar un archivo de configuración a un comando `certool`. Consulte Cambiar las opciones de configuración de certool. Consulte Reemplazar los certificados firmado por VMCA existentes por certificados nuevos firmados por VMCA mediante la CLI para ver algunos ejemplos de uso. La ayuda de la línea de comandos proporciona detalles sobre las opciones.

certool --initcsr

Genera una solicitud de firma de certificados (CSR). El comando genera un archivo PKCS10 y una clave privada.

Opción	Descripción
`--gencsr`	Se necesita para generar las CSR.
`--privkey <key_file>`	Nombre del archivo de clave privada.
`--pubkey <key_file>`	Nombre del archivo de clave pública.
`--csrfile <csr_file>`	Nombre del archivo de CSR que se enviará al proveedor de la entidad de certificación.
`--config <config_file>`	Nombre del archivo de configuración. Un archivo de configuración de ejemplo se encuentra en `/usr/lib/vmware-vmca/share/config/certool.cfg`. Como práctica recomendada, haga una copia del archivo de configuración predeterminado y reemplace los campos obligatorios.

Ejemplo:

```
certool --gencsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

Crea un certificado autofirmado y aprovisiona el servidor de VMCA con una entidad de certificación raíz autofirmada. Esta opción es una de las formas más simples de aprovisionar el servidor de VMCA. Otra opción es aprovisionar el servidor VMCA con un certificado raíz externo de modo que VMCA sea una entidad de certificación intermedia. Consulte Convertir VMCA en una entidad de certificación intermedia mediante la CLI.

Este comando genera un certificado con la fecha establecida tres días antes para evitar conflictos entre las zonas horarias.

Opción	Descripción
`--selfca`	Se necesita para generar un certificado autofirmado.
`--predate <number_of_minutes>`	Permite establecer el campo No válido hasta del certificado raíz en la cantidad de minutos determinada antes de la hora actual. Esta opción puede resultar útil para dar cuenta de posibles problemas con las zonas horarias. El valor máximo es tres días.
`--config <config_file>`	Nombre del archivo de configuración. Un archivo de configuración de ejemplo se encuentra en `/usr/lib/vmware-vmca/share/config/certool.cfg`. Como práctica recomendada, haga una copia del archivo de configuración predeterminado y reemplace los campos obligatorios.
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

certool --rootca

Importa un certificado raíz. Agrega el certificado especificado y la clave privada a VMCA. VMCA usa siempre el certificado raíz más reciente para la firma, pero pueden quedar otros certificados raíz de confianza hasta que los elimina manualmente. Esto significa que el usuario puede actualizar la infraestructura un paso a la vez y, por último, eliminar los certificados que ya no use.

Opción	Descripción
`--rootca`	Se necesita para importar una entidad de certificación raíz.
`--cert <certfile>`	Nombre del archivo de certificado.

Opción	Descripción
`--privkey <key_file>`	Nombre del archivo de clave privada. Este archivo debe estar en el formato codificado PEM.
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

Devuelve el nombre de dominio predeterminado que usa vmdir.

Opción	Descripción
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.
`--port <port_num>`	Número de puerto opcional. El valor predeterminado es el puerto 389.

Ejemplo:

```
certool --getdc
```

certool --waitVMDIR

Espere a que VMware Directory Service se ejecute o a que se cumpla el tiempo de espera especificado por `--wait`. Use esta opción, junto con otras opciones, para programar determinadas tareas, como obtener el nombre de dominio predeterminado.

Opción	Descripción
`--wait`	Cantidad opcional de minutos para esperar. El valor predeterminado es 3.
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.
`--port <port_num>`	Número de puerto opcional. El valor predeterminado es el puerto 389.

Ejemplo:

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

Espere a que el servicio VMCA se ejecute o a que se cumpla el tiempo de espera especificado. Use esta opción, junto con otras opciones, para programar determinadas tareas, como generar un certificado.

Opción	Descripción
`--wait`	Cantidad opcional de minutos para esperar. El valor predeterminado es 3.
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.
`--port <port_num>`	Número de puerto opcional. El valor predeterminado es el puerto 389.

Ejemplo:

```
certool --waitVMCA --selfca
```

certool --publish-roots

Fuerza la actualización de certificados raíz. Este comando requiere privilegios administrativos.

Opción	Descripción
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --publish-roots
```

Referencia de comandos de administración de certool

Los comandos de administración `certool` permiten ver, generar y revocar certificados, y ver información sobre ellos.

certool --genkey

Genera un par de claves privada y pública. Estos archivos se pueden utilizar para generar un certificado firmado por VMCA.

Opción	Descripción
`--genkey`	Se requiere para generar una clave privada y pública.
`--privkey <keyfile>`	Nombre del archivo de clave privada.

Opción	Descripción
--pubkey <keyfile>	Nombre del archivo de clave pública.
--server <server>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

Genera un certificado desde el servidor de VMCA. Este comando utiliza la información de certool.cfg o del archivo de configuración especificado. Puede usar el certificado para aprovisionar certificados de máquinas o certificados de usuarios de solución.

Opción	Descripción
--gencert	Se requiere para generar un certificado.
--cert <certfile>	Nombre del archivo de certificado. Este archivo debe estar en el formato codificado PEM.
--privkey <keyfile>	Nombre del archivo de clave privada. Este archivo debe estar en el formato codificado PEM.
--config <config_file>	Nombre del archivo de configuración. Un archivo de configuración de ejemplo se encuentra en /usr/lib/vmware-vmca/share/config/certool.cfg. Como práctica recomendada, haga una copia del archivo de configuración predeterminado y reemplace los campos obligatorios.
--server <server>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --gencert --privkey=<filename> --cert=<filename> --config=<config_file>
```

certool --getrootca

Imprime un certificado actual de la entidad de certificación raíz en formato de lenguaje natural. Esta salida no se puede utilizar como certificado porque está cambiada a lenguaje natural.

Opción	Descripción
--getrootca	Se requiere para imprimir el certificado raíz.
--server <server>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --getrootca --server=remoteserver
```

certool --viewcert

Imprime todos los campos de un certificado en formato de lenguaje natural.

Opción	Descripción
`--viewcert`	Se requiere para ver un certificado.
`--cert <certfile>`	Nombre del archivo de configuración. Un archivo de configuración de ejemplo se encuentra en `/usr/lib/vmware-vmca/share/config/certool.cfg`. Como práctica recomendada, haga una copia del archivo de configuración predeterminado y reemplace los campos obligatorios.

Ejemplo:

```
certool --viewcert --cert=<filename>
```

certool --enumcert

Enumera todos los certificados que conoce el servidor de VMCA. La opción `filter` (filtrar) permite enumerar todos los certificados o solo los certificados revocados, activos o caducados.

Opción	Descripción
`--enumcert`	Se requiere para enumerar todos los certificados.
`--filter [all | active]`	Filtro requerido. Especifique todos o los que están activos. Las opciones revocadas o caducadas no se admiten en este momento.

Ejemplo:

```
certool --enumcert --filter=active
```

certool --status

Envía un certificado especificado al servidor de VMCA para comprobar si está revocado. Se muestra `Certificado: REVOCADO` si se revoca el certificado; de lo contrario, `Certificado: ACTIVO`.

Opción	Descripción
--status	Se requiere para comprobar el estado de un certificado.
--cert <certfile>	Nombre del archivo de configuración. Un archivo de configuración de ejemplo se encuentra en /usr/lib/vmware-vmca/share/config/certool.cfg. Como práctica recomendada, haga una copia del archivo de configuración predeterminado y reemplace los campos obligatorios.
--server <server>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --status --cert=<filename>
```

certool --genselfcacert

Genera un certificado autofirmado a partir de los valores del archivo de configuración. Este comando genera un certificado con la fecha establecida tres días antes para evitar conflictos entre las zonas horarias.

Opción	Descripción
--genselfcacert	Se necesita para generar un certificado autofirmado.
--outcert <cert_file>	Nombre del archivo de certificado. Este archivo debe estar en el formato codificado PEM.
--outprivkey <key_file>	Nombre del archivo de clave privada. Este archivo debe estar en el formato codificado PEM.
--config <config_file>	Nombre del archivo de configuración. Un archivo de configuración de ejemplo se encuentra en /usr/lib/vmware-vmca/share/config/certool.cfg. Como práctica recomendada, haga una copia del archivo de configuración predeterminado y reemplace los campos obligatorios.

Ejemplo:

```
certool --genselfcert --privkey=<filename> --cert=<filename> --config=<config_file>
```

Referencia de comandos vecs-cli

El conjunto de comandos vecs-cli permite administrar las instancias de VMware Certificate Store (VECS). Utilice estos comandos junto con dir-cli y certool para administrar la infraestructura de certificados y los servicios de autenticación.

vecs-cli store create

Crea un almacén de certificados.

Opción	Descripción
`--name <name>`	Nombre del almacén de certificados.
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

Ejemplo:

```
vecs-cli store create --name <store>
```

vecs-cli store delete

Elimina un almacén de certificados. Puede eliminar los almacenes del sistema MACHINE_SSL_CERT, TRUSTED_ROOTS y TRUSTED_ROOT_CRLS. Los usuarios con privilegios exigidos pueden eliminar los almacenes de usuarios de solución.

Opción	Descripción
`--name <name>`	Nombre del almacén de certificados que se va a eliminar.
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

Ejemplo:

```
vecs-cli store delete --name <store>
```

vecs-cli store list

Enumera los almacenes de certificados.

Opción	Descripción
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

VECS incluye los siguientes almacenes.

Tabla 3-2. Almacenes en VECS

Almacén	Descripción
Almacén SSL de máquina (MACHINE_SSL_CERT)	■ El servicio de proxy inverso lo utiliza en cada nodo de vSphere. ■ VMware Directory Service (vmdir) lo utiliza en cada nodo de vCenter Server. Todos los servicios de vSphere 6.0 y versiones posteriores se comunican mediante un proxy inverso que utiliza el certificado SSL de equipo. Por razones de compatibilidad con versiones anteriores, los servicios de la versión 5.x todavía utilizan puertos específicos. Como resultado, algunos servicios como vpxd todavía tienen su propio puerto abierto.
Almacenes de usuarios de solución ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	VECS incluye un almacén para cada usuario de solución. El asunto de cada certificado de usuario de solución debe ser único, por ejemplo, el certificado de máquina no puede tener el mismo asunto que el certificado de vpxd. Los certificados de usuarios de solución se utilizan para efectuar la autenticación con vCenter Single Sign-On. vCenter Single Sign-On comprueba que el certificado sea válido, pero no comprueba otros atributos del certificado. En VECS, se incluyen los siguientes almacenes de certificados de usuarios de solución: ■ `machine`: lo utilizan el servidor de licencias y el servicio de registro. **Nota** El certificado de usuario de solución de la máquina no tiene relación alguna con el certificado SSL de máquina. El certificado de usuario de solución de la máquina se utiliza para el intercambio de tokens SAML, mientras que el certificado SSL de máquina se utiliza para las conexiones SSL seguras de una máquina. ■ `vpxd`: almacén de daemon del servicio vCenter (vpxd). vpxd utiliza el certificado de usuario de solución que está almacenado en este almacén para autenticarse en vCenter Single Sign-On. ■ `vpxd-extension`: almacén de extensiones de vCenter. Incluye el servicio de Auto Deploy, el servicio de inventario u otros servicios que no forman parte de otros usuarios de solución. ■ `vsphere-webclient`: almacén de vSphere Client. También incluye algunos servicios adicionales como el servicio de gráficos de rendimiento. ■ `wcp`: VMware vSphere® con almacén de VMware Tanzu™. También se utiliza para vSphere Cluster Services. Cada nodo de vCenter Server incluye un certificado `machine`.
Almacén raíz de confianza (TRUSTED_ROOTS)	Contiene todos los certificados raíz de confianza.

Tabla 3-2. Almacenes en VECS (continuación)

Almacén	Descripción
Almacén de copias de seguridad de la utilidad vSphere Certificate Manager (BACKUP_STORE)	VMCA (VMware Certificate Manager) lo utiliza para admitir la reversión de certificados. Solo el estado más reciente se almacena como copia de seguridad; no se puede volver más de un paso.
Otros almacenes	Las soluciones pueden agregar otros almacenes. Por ejemplo, la solución Virtual Volumes agrega un almacén SMS. No modifique los certificados de estos almacenes a menos que así se indique en la documentación de VMware o en un artículo de la base de conocimientos de VMware. **Nota** La eliminación del almacén TRUSTED_ROOTS_CRLS puede dañar la infraestructura de certificado. No elimine ni modifique el almacén TRUSTED_ROOTS_CRLS.

Ejemplo:

```
vecs-cli store list
```

vecs-cli store permissions

Otorga o revoca permisos en el almacén. Utilice la opción --grant o --revoke.

El propietario de almacén puede realizar todas las operaciones, incluso otorgar y revocar permisos. El administrador del dominio local de vCenter Single Sign-On, administrator@vsphere.local de manera predeterminada, tiene todos los privilegios en todos los almacenes, incluso otorgar y revocar permisos.

Se puede utilizar vecs-cli get-permissions --name <store-name> para recuperar la configuración actual del almacén.

<table>
<tr><th>Opción</th><th>Descripción</th></tr>
<tr><td>--name <name></td><td>Nombre del almacén de certificados.</td></tr>
<tr><td>--user <username></td><td>Nombre único del usuario al que se otorgan permisos.</td></tr>
<tr><td>--grant [read|write]</td><td>Permiso que se va a otorgar, ya sea de lectura o de escritura.</td></tr>
<tr><td>--revoke [read|write]</td><td>Permiso que se va a revocar, ya sea de lectura o de escritura. No es compatible en este momento.</td></tr>
</table>

vecs-cli store get-permissions

Recupera la configuración de permiso actual para el almacén.

Opción	Descripción
--name <name>	Nombre del almacén de certificados.
--server <server-name>	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
--upn <user-name>	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por --server <server-name> . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

vecs-cli entry create

Crea una entrada en VECS. Utilice este comando para agregar una clave privada o un certificado a un almacén.

Nota No utilice este comando para agregar certificados raíz al almacén de TRUSTED_ROOTS. En su lugar, utilice el comando dir-cli para publicar estos certificados.

Opción	Descripción
--store <NameOfStore>	Nombre del almacén de certificados.
--alias <Alias>	Alias opcional del certificado. Esta opción se ignora para el almacén raíz de confianza.
--cert <certificate_file_path>	Ruta de acceso completa del archivo de certificado.
--key <key-file-path>	Ruta de acceso completa de la clave que corresponde al certificado. Opcional.
--password <password>	Contraseña opcional para cifrar la clave privada.
--server <server-name>	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
--upn <user-name>	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por --server <server-name> . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

vecs-cli entry list

Enumera todas las entradas en un almacén especificado.

Opción	Descripción
--store <NameOfStore>	Nombre del almacén de certificados.

vecs-cli entry getcert

Recupera un certificado de VECS. Es posible enviar el certificado en un archivo de salida o mostrarlo como texto en lenguaje natural.

Opción	Descripción
`--store <NameOfStore>`	Nombre del almacén de certificados.
`--alias <Alias>`	Alias del certificado.
`--output <output_file_path>`	Archivo donde se escribe el certificado.
`--text`	Muestra una versión del certificado en lenguaje natural.
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

vecs-cli entry getkey

Recupera una clave almacenada en VECS. Es posible enviar la clave en un archivo de salida o mostrarla como texto en lenguaje natural.

Opción	Descripción
`--store <NameOfStore>`	Nombre del almacén de certificados.
`--alias <Alias>`	Alias de la clave.
`--output <output_file_path>`	Archivo de salida donde se escribe la clave.
`--text`	Muestra una versión de la clave en lenguaje natural.
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

vecs-cli entry delete

Elimina una entrada de un almacén de certificados. Si se elimina una entrada en VECS, esta se quita de forma permanente de VECS. La única excepción es el certificado raíz actual. VECS sondea vmdir en busca de un certificado raíz.

Opción	Descripción
`--store <NameOfStore>`	Nombre del almacén de certificados.
`--alias <Alias>`	Alias de la entrada que se desea eliminar.
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.
`-y`	Suprime la solicitud de confirmación. Para usuarios avanzados solamente.

vecs-cli force-refresh

Fuerza una actualización de VECS. De forma predeterminada, VECS sondea vmdir cada 5 minutos en busca de archivos de certificado raíz nuevos. Utilice este comando para realizar una actualización inmediata de VECS desde vmdir.

Opción	Descripción
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

Referencia de comando dir-cli

La utilidad `dir-cli` admite la creación y actualización de usuarios de solución, administración de cuentas y administración de certificados y contraseñas en VMware Directory Service (vmdir). Puede usar `dir-cli` para administrar y consultar el nivel funcional de dominio de las instancias de vCenter Server.

dir-cli nodes list

Enumera todos los sistemas vCenter Server conectados de Enhanced Linked Mode.

Opción	Descripción
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.
--server <psc_ip_or_fqdn>	Utilice esta opción para conectarse a otra instancia de vCenter Server para ver sus socios de replicación.

dir-cli computer password-reset

Permite restablecer la contraseña de la cuenta de máquina en el dominio.

Opción	Descripción
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.
--live-dc-hostname <server name>	Nombre actual de la instancia de vCenter Server.

dir-cli service create

Crea un usuario de solución. Se usa sobre todo en soluciones externas.

Opción	Descripción
--name <name>	Nombre del usuario de solución que se va a crear
--cert <cert file>	Ruta de acceso al archivo de certificado. Puede ser un certificado firmado por VMCA o un certificado externo.
--ssogroups <comma-separated-groupnames>	Incluye al usuario de la solución como miembro de los grupos especificados.
--wstrustrole <ActAsUser>	Incluye al usuario de la solución como miembro del grupo integrado de administradores o usuarios. En otras palabras, determina si el usuario de la solución tiene privilegios administrativos.
--ssoadminrole <Administrator/User>	Incluye al usuario de la solución como miembro del grupo ActAsUser. La función ActAsUser permite a los usuarios actuar en nombre de otros usuarios.
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli service list

Enumera a los usuarios de solución que conoce `dir-cli`.

Opción	Descripción
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli service delete

Elimina un usuario de solución en vmdir. Cuando se elimina el usuario de solución, todos los servicios asociados dejan de estar disponibles en los nodos de administración que usan esta instancia de vmdir.

Opción	Descripción
`--name`	Nombre del usuario de solución que se va a eliminar.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli service update

Actualiza el certificado de un usuario de solución especificado, es decir, de una recopilación de servicios. Después de ejecutar este comando, actualice la entrada del certificado de usuario de solución en VECS ejecutando el comando `vecs-cli entry create`. Consulte Referencia de comandos vecs-cli.

Opción	Descripción
`--name <name>`	Nombre del usuario de solución que se va a actualizar.
`--cert <cert_file>`	Nombre del certificado que se va a asignar al servicio.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli user create

Crea un usuario regular en vmdir. Este comando puede usarse para usuarios humanos que se autentican en vCenter Single Sign-On con un nombre de usuario y una contraseña. Use este comando únicamente durante la creación de prototipos.

Opción	Descripción
`--account <name>`	Nombre del usuario de vCenter Single Sign-On que se va a crear.
`--user-password <password>`	Contraseña inicial del usuario.
`--first-name <name>`	Nombre de pila del usuario.
`--last-name <name>`	Apellido del usuario.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli user modify

Modifica el usuario especificado dentro de vmdir.

Opción	Descripción
`--account <name>`	Nombre del usuario de vCenter Single Sign-On que se va a modificar.
`--password-never-expires`	Esta opción se establece en true si va a modificar una cuenta de usuario para tareas automatizadas que deben autenticarse en vCenter Server y desea asegurarse de que no se detenga la ejecución de las tareas por caducidad de contraseñas. Utilice con atención esta opción.
`--password-expires`	Esta opción se establece en true si desea revertir la opción `--password-never-expires`.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli user delete

Elimina el usuario especificado en vmdir.

Opción	Descripción
`--account <name>`	Nombre del usuario de vCenter Single Sign-On que se va a eliminar.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli user find-by-name

Busca usuarios por nombre en vmdir. La información que devuelve este comando depende de lo que se especifique en la opción `--level`.

Opción	Descripción
`--account <name>`	Nombre del usuario de vCenter Single Sign-On que se va a buscar.
`--level <info level 0|1|2>`	Devuelve la siguiente información: ■ Nivel 0: cuenta y UPN ■ Nivel 1: información del nivel 0 + nombre y apellido ■ Nivel 2: nivel 0 + marca de cuenta desactivada, marca de cuenta bloqueada, marca de contraseña sin fecha de caducidad, marca de contraseña caducada y marca de caducidad de contraseña. El nivel predeterminado es 0.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli group modify

Agrega un usuario o un grupo a un grupo que ya existe.

Opción	Descripción
`--name <name>`	Nombre del grupo en vmdir.
`--add <user_or_group_name>`	Nombre del usuario o el grupo que se va a agregar.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli group list

Enumera un grupo de vmdir específico.

Opción	Descripción
`--name <name>`	Nombre opcional del grupo en vmdir. Esta opción permite comprobar si existe un grupo específico.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli ssogroup create

Crea un grupo en el dominio local (vsphere.local de forma predeterminada).

Use este comando si desea crear grupos para administrar los permisos del usuario en el dominio de vCenter Single Sign-On. Por ejemplo, si crea un grupo y luego lo agrega al grupo Administradores del dominio de vCenter Single Sign-On, todos los usuarios que agregue al grupo tendrán permisos de administrador en el dominio.

También es posible otorgar permisos para los objetos de inventario de vCenter a los grupos del dominio de vCenter Single Sign-On. Consulte la documentación de *Seguridad de vSphere*.

Opción	Descripción
`--name <name>`	Nombre del grupo en vmdir. La longitud máxima es de 487 caracteres.
`--description <description>`	Descripción opcional para el grupo.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli trustedcert publish

Publica un certificado raíz de confianza en vmdir. Después de ejecutar este comando, VECS selecciona el cambio de certificado después de un minuto, o bien puede ejecutar el comando `vecs-cli force-refresh` para sincronizar el certificado inmediatamente.

Nota A partir de vSphere 8.0 Update 3, utilice el vSphere Client o la API para publicar un certificado raíz de confianza y así evitar tener que reiniciar los servicios.

Opción	Descripción
`--cert <file>`	Ruta de acceso al archivo de certificado.
`--crl <file>`	Esta opción no es compatible con VMCA.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.
`--chain`	Especifique esta opción si va a publicar un certificado encadenado. No se requiere ningún valor de opción.

dir-cli trustedcert unpublish

Anula la publicación de un certificado raíz de confianza que actualmente está en vmdir. Utilice este comando, por ejemplo, si agregó un certificado raíz diferente a vmdir que es ahora el certificado raíz de todos los otros certificados del entorno. La anulación de la publicación de los certificados que ya no se utilizan forma parte del fortalecimiento del entorno.

Nota A partir de vSphere 8.0 Update 3, utilice el vSphere Client o la API para cancelar la publicación de un certificado raíz de confianza y así evitar tener que reiniciar los servicios.

Opción	Descripción
`--cert-file <file>`	Ruta de acceso al archivo de certificado cuya publicación se va a anular.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli trustedcert list

Enumera todos los certificados raíz de confianza y sus correspondientes identificadores Los identificadores de los certificados son necesarios para recuperar un certificado con `dir-cli trustedcert get`.

Opción	Descripción
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli trustedcert get

Recupera un certificado raíz de confianza desde vmdir y lo escribe en un archivo especificado.

Opción	Descripción
`--id <cert_ID>`	Identificador del certificado que se va a recuperar. El comando `dir-cli trustedcert list` muestra el identificador.
`--outcert <path>`	Ruta de acceso donde se escribe el archivo de certificado.
`--outcrl <path>`	Ruta de acceso donde se escribe el archivo CRL. No se encuentra en uso.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli password create

Crea una contraseña aleatoria que cumple con los requisitos de contraseñas. Este comando puede ser utilizado por usuarios de solución externa.

Opción	Descripción
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli password reset

Permite que un administrador restablezca la contraseña de un usuario. Si usted es un usuario sin permisos de administrador y desea restablecer una contraseña, utilice el comando `dir-cli password change`.

Opción	Descripción
`--account`	Nombre de la cuenta a la que se le asignará una nueva contraseña.
`--new`	Nueva contraseña del usuario especificado.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli password change

Le permite a un usuario cambiar su contraseña. Es necesario ser el usuario propietario de la cuenta para poder hacer este cambio. Los administradores pueden utilizar el comando `dir-cli password reset` para restablecer cualquier contraseña.

Opción	Descripción
`--account`	Nombre de la cuenta.
`--current`	Contraseña actual del usuario propietario de la cuenta.
`--new`	Nueva contraseña del usuario propietario de la cuenta.

Autenticar vSphere con vCenter Single Sign-On

4

vCenter Single Sign-On es un agente de autenticación y una infraestructura de intercambio de tokens de seguridad. vCenter Single Sign-On emite un token cuando se autentica un usuario. El usuario puede utilizar el token para autenticarse en los servicios de vCenter Server. Luego, el usuario puede realizar las acciones para las que tiene privilegios.

Ya que el tráfico está cifrado para todas las comunicaciones y solo los usuarios autenticados puede realizar las acciones para las que tienen privilegios, el entorno permanece seguro.

Los usuarios y las cuentas de servicio se autentican con un token, o con un nombre de usuario y una contraseña. Los usuarios de solución se autentican con un certificado. Para obtener información sobre el reemplazo de certificados de usuarios de solución, consulte Capítulo 2 Certificados de seguridad de vSphere.

El siguiente paso es autorizar a los usuarios que pueden autenticar a que realicen ciertas tareas. Por lo general, se asignan privilegios de vCenter Server y, para ello, se suele asignar el usuario a un grupo con una función. vSphere incluye otros modelos de permiso como permisos globales. Consulte la documentación de *Seguridad de vSphere*.

Lea los siguientes temas a continuación:

- Cómo vCenter Single Sign-On protege el entorno
- vCenter Server Federación de proveedor de identidad
- Federación de proveedores de identidad de vCenter Server y Enhanced Linked Mode
- Configurar la federación de proveedores de identidad de vCenter Server
- vCenter Single Sign-On
- Configurar orígenes de identidad de vCenter Single Sign-On
- Administrar el servicio de token de seguridad de vCenter Server
- Administrar directivas de vCenter Single Sign-On
- Administrar usuarios y grupos de vCenter Single Sign-On
- Opciones de autenticación de vSphere
- Administrar el mensaje de inicio de sesión en la página de inicio de sesión de vSphere Client
- Prácticas recomendadas de seguridad de vCenter Single Sign-On

Cómo vCenter Single Sign-On protege el entorno

vCenter Single Sign-On permite que los componentes de vSphere se comuniquen entre sí a través de un mecanismo de token seguro.

vCenter Single Sign-On utiliza los siguientes servicios.

- Autenticación de usuarios a través de la federación de proveedores de identidad externo o el proveedor de identidad integrado de vCenter Server. El proveedor de identidad integrado admite cuentas locales, Active Directory u OpenLDAP, autenticación de Windows integrada (IWA) y mecanismos de autenticación diversos (tarjeta inteligente y RSA SecurID).
- La autenticación de usuarios de soluciones a través de certificados.
- Servicio de token de seguridad (Security Token Service, STS).
- SSL para proteger el tráfico.

Proveedor de identidad integrado de vCenter Server

vCenter Server incluye un proveedor de identidad integrado. De forma predeterminada, vCenter Server utiliza el dominio vsphere.local como el origen de identidad (pero puede cambiar el dominio durante la instalación). Puede configurar el proveedor de identidad integrado de vCenter Server para que utilice Active Directory (AD) como su origen de identidad mediante LDAP/S, OpenLDAP/S y la autenticación de Windows integrada (IWA). Estas configuraciones permiten a los clientes iniciar sesión en vCenter Server a través de sus cuentas de AD.

vCenter Server y un proveedor de identidad externo

En vSphere 7.0 y versiones posteriores, puede configurar vCenter Server para un proveedor de identidad externo mediante la autenticación federada. En una configuración de este tipo, debe reemplazar a vCenter Server como el proveedor de identidad.

vSphere admite los siguientes proveedores de identidad.

- vSphere 7.0 y versiones posteriores: Active Directory Federation Services (AD FS)
- vSphere 8.0 Update 1 y versiones posteriores: Okta
- vSphere 8.0 Update 2 y versiones posteriores: Microsoft Entra ID (anteriormente denominado Azure AD)
- A partir de vSphere 8.0 Update 3: PingFederate

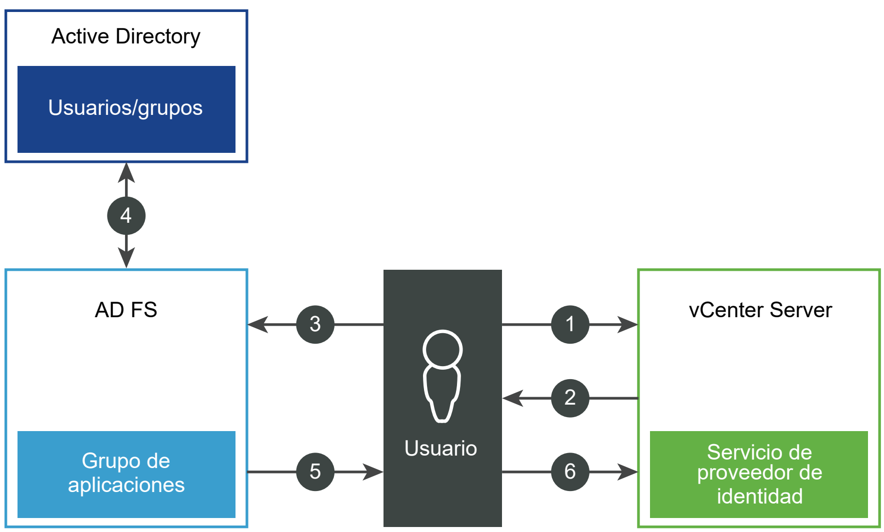
Cuando se configura vSphere para utilizar un proveedor de identidad externo, este interactúa con los orígenes de identidad en nombre de vCenter Server.

Inicio de sesión del usuario con autenticación federada del proveedor de identidad de vCenter Server

Cuando se utiliza un proveedor de identidad externo para autenticarse con la instancia de vCenter Server, la instancia de vCenter Server redirecciona la solicitud de inicio de sesión al proveedor de identidad externo. El proveedor de identidad externo autentica al usuario con su servicio de directorio y, a continuación, emite un token para que vCenter Server lo utilice a fin de iniciar sesión en el usuario.

Por ejemplo, la siguiente figura muestra una vista detallada del flujo de inicio de sesión de usuario para la federación de proveedores de identidad de vCenter Server mediante AD FS.

Figura 4-1. Inicio de sesión de usuario en vCenter Server mediante la federación de proveedores de identidad AD FS



vCenter Server, AD FS y Active Directory interactúan de la siguiente manera:

1 El usuario comienza en la página de destino de vCenter Server e introduce allí un nombre de usuario.

2 Si el nombre de usuario es para un dominio federado, vCenter Server redirecciona la solicitud de autenticación a AD FS.

3 Si es necesario, AD FS solicita al usuario que inicie sesión con las credenciales de Active Directory.

4 AD FS autentica al usuario con Active Directory.

5 AD FS emite un token de seguridad con información de grupo de Active Directory.

6 vCenter Server utiliza el token para iniciar la sesión del usuario.

Ahora el usuario está autenticado, y puede ver y modificar todos los objetos sobre los que tiene privilegios por su función.

Nota Al principio, se asigna la función Sin acceso a cada usuario. Un administrador de vCenter Server debe asignar al menos la función Solo lectura al usuario para que pueda iniciar sesión. Consulte la documentación de *Seguridad de vSphere*.

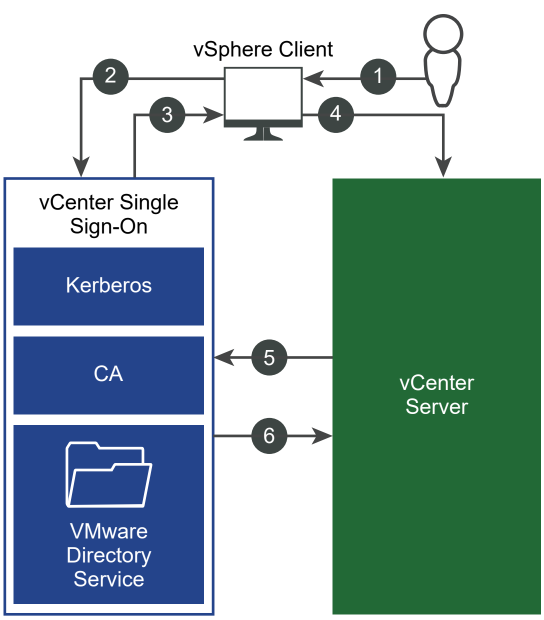
En caso de que no se pueda acceder al proveedor de identidad externo, el proceso de inicio de sesión vuelve a la página de destino de vCenter Server, donde se muestra un mensaje de información adecuado. Los usuarios también pueden iniciar sesión con sus cuentas locales en el origen de identidad vsphere.local.

La interacción entre vCenter Server y Okta, Microsoft Entra ID o PingFederate es similar a la de AD FS, con la excepción de que vCenter Server utiliza VMware Identity Services. Consulte Proceso de autenticación de VMware Identity Services.

Inicio de sesión del usuario con el proveedor de identidad integrado de vCenter Server

En la siguiente figura, se muestra el flujo de inicio de sesión del usuario cuando vCenter Server actúa como el proveedor de identidad.

Figura 4-2. Inicio de sesión del usuario con el proveedor de identidad integrado de vCenter Server



1 El usuario inicia sesión en vSphere Client con un nombre de usuario y una contraseña para acceder al sistema vCenter Server o a otro servicio de vCenter.

2 vSphere Client pasa la información de inicio de sesión al servicio vCenter Single Sign-On, que comprueba el token SAML de vSphere Client. Si vSphere Client tiene un token válido, vCenter Single Sign-On comprueba si el usuario se encuentra en el origen de identidad configurado (por ejemplo, Active Directory).

   - Si solo se emplea el nombre de usuario, vCenter Single Sign-On comprueba el dominio predeterminado.
   - Si se incluye un nombre de dominio con el nombre de usuario (*DOMAIN*\user1 o user1@*DOMAIN*), vCenter Single Sign-On comprueba ese dominio.

3 Si el usuario puede autenticarse en el origen de identidad, vCenter Single Sign-On devuelve un token que representa al usuario en vSphere Client.

4 vSphere Client pasa el token al sistema vCenter Server.

5 vCenter Server comprueba con el servidor de vCenter Single Sign-On que el token sea válido y que no haya caducado.

6 El servidor de vCenter Single Sign-On devuelve el token al sistema vCenter Server mediante el marco de autorización de vCenter Server para otorgar acceso a los usuarios.

Ahora el usuario está autenticado, y puede ver y modificar todos los objetos sobre los que tiene privilegios por su función.

Nota Al principio, se asigna la función Sin acceso a cada usuario. Un administrador de vCenter Server debe asignar al menos la función Solo lectura al usuario para que pueda iniciar sesión. Consulte la documentación de *Seguridad de vSphere*.

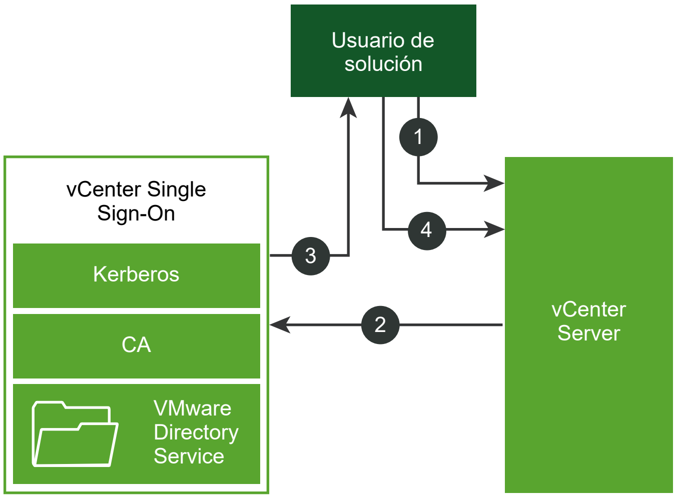
Inicio de sesión para usuarios de solución

Los usuarios de solución son conjuntos de servicios que se usan en la infraestructura de vCenter Server, por ejemplo, las extensiones de vCenter Server. Las extensiones de VMware y las posibles extensiones externas también pueden autenticarse en vCenter Single Sign-On.

Nota vCenter Server utiliza certificados de usuarios de solución solo para comunicación interna. Los certificados de usuarios de solución no se utilizan para la comunicación externa.

En la siguiente figura, se muestra el flujo de inicio de sesión para usuarios de solución.

Figura 4-3. Inicio de sesión para usuarios de solución



1 El usuario de solución intenta conectarse a un servicio de vCenter Server.

2 Se redirige al usuario de solución a vCenter Single Sign-On. Si el usuario de solución es nuevo en vCenter Single Sign-On, debe presentar un certificado válido.

3 Si el certificado es válido, vCenter Single Sign-On asigna un token SAML (token de portador) al usuario de solución. vCenter Single Sign-On firma el token.

4 El usuario de solución se redirige a vCenter Single Sign-On y puede realizar tareas según sus permisos.

   La próxima vez que el usuario de solución deba autenticarse, podrá usar el token SAML para iniciar sesión en vCenter Server.

De forma predeterminada, este protocolo de enlace se aplica automáticamente, ya que VMCA aprovisiona a los usuarios de solución con certificados durante el inicio. Si la directiva de la empresa exige certificados externos firmados por una entidad de certificación, se pueden utilizar esos certificados para reemplazar los certificados de los usuarios de solución. Si esos certificados son válidos, vCenter Single Sign-On asigna un token SAML al usuario de solución. Consulte Reemplazar certificados de usuario de solución por certificados personalizados mediante el administrador de certificados.

Cifrado compatible en vSphere

Se admite el cifrado AES, que es el nivel más alto de cifrado. El cifrado compatible también afecta a la seguridad cuando vCenter Single Sign-On utiliza Active Directory como un origen de identidad.

También afecta a la seguridad cada vez que un host ESXi o vCenter Server se une a Active Directory.

vCenter Server Federación de proveedor de identidad

En vSphere 7.0 o versiones posteriores, vCenter Server admite la autenticación federada para iniciar sesión en vCenter Server.

Para habilitar la autenticación federada en vCenter Server, debe configurar una conexión con un proveedor de identidad externo. La instancia del proveedor de identidad que se configura reemplaza a vCenter Server como el proveedor de identidad. Actualmente, vCenter Server admite Active Directory Federation Services (AD FS), Okta, Microsoft Entra ID (anteriormente denominado Azure AD) y PingFederate como proveedores de identidad externos. vCenter Server admite AD FS en vSphere 7.0 y versiones posteriores, Okta en vSphere 8.0 Update 1 y versiones posteriores, Microsoft Entra ID en vSphere 8.0 Update 2 y versiones posteriores y PingFederate a partir de vSphere 8.0 Update 3.

Nota VMware recomienda utilizar la autenticación federada a medida que vSphere avanza hacia la autenticación basada en token. vCenter Server sigue teniendo cuentas locales para acceso administrativo y recuperación de errores.

Cómo funciona la federación de proveedores de identidad de vCenter Server

La federación de proveedores de identidad de vCenter Server le permite configurar un proveedor de identidad externo para autenticación federada. En esta configuración, el proveedor de identidad externo interactúa con el origen de identidad en nombre de vCenter Server.

Conceptos básicos de la federación de proveedores de identidad de vCenter Server

En vSphere 7.0 y versiones posteriores, vCenter Server admite la autenticación federada. En este escenario, cuando un usuario inicia sesión en vCenter Server, vCenter Server redirecciona el inicio de sesión del usuario al proveedor de identidad externo. Ya no se proporcionan las credenciales de usuario directamente a vCenter Server. En su lugar, el usuario proporciona las credenciales al proveedor de identidad externo. vCenter Server confía en el proveedor de identidad externo para realizar la autenticación. En el modelo de federación, los usuarios nunca proporcionan credenciales directamente a ningún servicio ni aplicación, sino solo al proveedor de identidad. Como resultado, con el proveedor de identidad puede "federar" las aplicaciones y los servicios, como vCenter Server.

Compatibilidad con proveedores de identidad externos de vCenter Server

vCenter Server admite los siguientes proveedores de identidad externos:

- AD FS (vSphere 7.0 y versiones posteriores)
- Okta (vSphere 8.0 Update 1 y versiones posteriores)
- Microsoft Entra ID, anteriormente denominado Azure AD (vSphere 8.0 Update 2 y versiones posteriores)

- PingFederate (a partir de vSphere 8.0 Update 3)

Ventajas de la federación de proveedores de identidad de vCenter Server

La federación de proveedores de identidad de vCenter Server proporciona las siguientes ventajas.

- Puede utilizar Single Sign-On con las aplicaciones y la infraestructura federada existentes.
- Puede mejorar la seguridad del centro de datos porque vCenter Server no controla nunca las credenciales del usuario.
- Puede utilizar mecanismos de autenticación, como la autenticación multifactor, compatible con el proveedor de identidad externo.

Arquitectura de la federación de proveedores de identidad de vCenter Server

Para establecer una relación de confianza entre vCenter Server y un proveedor de identidad externo, debe establecer la información de identificación y un secreto compartido entre ellos. vCenter Server usa el protocolo OpenID Connect (OIDC) para recibir un token de identidad que autentique al usuario con vCenter Server.

Los pasos detallados para configurar un proveedor de identidad externo con vCenter Server incluyen:

1. Establecer una confianza de usuario autenticado entre vCenter Server y el proveedor de identidad externo mediante la creación de una configuración de OIDC. Para AD FS, cree un grupo de aplicaciones o una aplicación. Para Okta, Microsoft Entra ID y PingFederate, cree una aplicación nativa con OpenID Connect como método de inicio de sesión. La configuración de OIDC consta de una aplicación de servidor y una API de Web. Los dos componentes especifican la información que vCenter Server usa para confiar y comunicarse con el proveedor de identidad externo.
2. Crear un proveedor de identidad correspondiente en vCenter Server.
3. Configurar la pertenencia a grupos en vCenter Server para autorizar el inicio de sesión de usuarios en el dominio del proveedor de identidad externo.

El administrador del proveedor de identidad debe proporcionar la siguiente información para crear la configuración del proveedor de identidad de vCenter Server:

- Identificador del cliente: la cadena UUID que se genera en AD FS al crear el grupo de aplicaciones (o la aplicación) y que identifica al grupo de aplicaciones (o la aplicación), o bien que se genera en Okta, Microsoft Entra ID o PingFederate al crear la aplicación OpenID Connect.
- Secreto compartido: el secreto que se genera en AD FS al crear el grupo de aplicaciones (o la aplicación) o que se genera en Okta, Microsoft Entra ID o PingFederate al crear la aplicación de OpenID Connect y que se utiliza para autenticar vCenter Server con el proveedor de identidad externo.

- Dirección de OpenID: la dirección URL del endpoint de detección de proveedores de OpenID correspondiente al servidor del proveedor de identidad externo, que especifica una dirección conocida que suele ser el endpoint del emisor concatenado con la ruta de acceso `/.well-known/openid-configuration`. A continuación se muestra un ejemplo de dirección de OpenID para una configuración de AD FS:

  ```
  https://webserver.example.com/adfs/.well-known/openid-configuration
  ```

  Del mismo modo, a continuación se muestra un ejemplo de dirección de OpenID para una configuración de Okta:

  ```
  https://example.okta.com/oauth2/default/.well-known/openid-configuration
  ```

  A continuación se muestra un ejemplo de dirección de OpenID para una configuración de Microsoft Entra ID:

  ```
  https://login.microsoftonline.com/11111111-2222-3333-4444-555555555555/v2.0/.well-known/
  openid-configuration
  ```

  A continuación se muestra un ejemplo de dirección de OpenID para una configuración de PingFederate:

  ```
  https://pingfederate-fqdn-and-port/.well-known/openid-configuration
  ```

VMware Identity Services y autenticación federada

En vSphere 8.0 Update 1 y versiones posteriores, VMware Identity Services proporciona una integración con los proveedores de identidad externos como proveedores de identidad federados. Puede pensar en la VMware Identity Services como una versión "reducida" de VMware Workspace ONE que está integrada en vSphere.

Al actualizar a vSphere 8.0 Update 1 o una versión posterior, o bien al instalarlo, VMware Identity Services se activa de forma predeterminada en vCenter Server. Al configurar Okta, Microsoft Entra ID o PingFederate como proveedores de identidad externos, vCenter Server utiliza VMware Identity Services para comunicarse con el servidor de Okta, Microsoft Entra ID o PingFederate.

vCenter Server admite Okta, Microsoft Entra ID y PingFederate como proveedores de identidad externos en una configuración de Enhanced Linked Mode. A pesar de que, en este tipo de configuración, varios sistemas de vCenter Server ejecutan VMware Identity Services, solo una instancia de vCenter Server y su instancia de VMware Identity Services se comunican con el servidor proveedor de identidad externo. Por ejemplo, si tiene una configuración de Enhanced Linked Mode de tres sistemas de vCenter Server (A, B y C) y configura el proveedor de identidad de Okta en vCenter Server A, vCenter Server A es el único sistema que controla todos los inicios de sesión de Okta. vCenter Server B y vCenter Server C no se comunican directamente con el

servidor Okta. Para configurar VMware Identity Services en otras instancias de vCenter Server de la configuración de ELM para interactuar con el servidor de IDP externo, consulte Proceso de activación para proveedores de identidad externos en configuraciones de Enhanced Linked Mode.

Nota Al configurar Okta como proveedor de identidad externo, todos los sistemas vCenter Server en una configuración de Enhanced Linked Mode deben ejecutar al menos vSphere 8.0 Update 1. Para Microsoft Entra ID, el requisito es al menos vSphere 8.0 Update 2. Para PingFederate, el requisito es al menos vSphere 8.0 Update 3.

Advertencia Cuando se utiliza una configuración de Enhanced Linked Mode con Okta, Microsoft Entra ID o PingFederate, no se puede eliminar la instancia de vCenter Server que ejecuta VMware Identity Services y que se comunica con el proveedor de identidad desde la configuración de ELM.

Proceso de autenticación de VMware Identity Services

Al configurar vCenter Server para utilizar VMware Identity Services a fin de comunicarse con el proveedor de identidad externo, se produce el siguiente proceso de autenticación:

1 Un usuario inicia sesión en vCenter Server con vSphere Client.

2 vCenter Single Sign-On delega la autenticación del usuario y redirecciona la solicitud de usuario a VMware Identity Services.

3 El proceso de VMware Identity Services solicita un token del proveedor de identidad externo para establecer la sesión de usuario.

4 El proveedor de identidad externo autentica al usuario (puede usar la autenticación multifactor [MFA] o las credenciales de SSO) y devuelve el token a VMware Identity Services.

   El token contiene las notificaciones de usuario.

5 El proceso de VMware Identity Services valida el token del proveedor de identidad, genera un token de VMware Identity Services correspondiente y lo envía a vCenter Single Sign-On.

6 vCenter Single Sign-On valida el token y concede la solicitud de inicio de sesión.

Nota AD FS no utiliza VMware Identity Services para la autenticación federada.

Cómo interactúa vCenter Server con usuarios y grupos insertados por SCIM

Al configurar su proveedor de identidad externo, vCenter Server utiliza el sistema para la administración de identidades entre dominios (SCIM) a fin de administrar usuarios y grupos. SCIM es un estándar abierto para automatizar el intercambio de información de identidad de usuario. Una aplicación de SCIM que crea en el servidor de IDP externo administra los usuarios y los grupos en el proveedor de identidad externo que desea insertar en vCenter Server. vCenter Server también utiliza SCIM al buscar usuarios y grupos para asignar permisos a objetos de vCenter Server.

Nota Una configuración de AD FS busca en Active Directory mediante LDAP. No utiliza SCIM.

Componentes de la federación de proveedores de identidad de vCenter Server

Los siguientes componentes incluyen una configuración de federación de proveedores de identidad de vCenter Server:

- Un vCenter Server
  - Para AD FS: vCenter Server 7.0 o versiones posteriores
  - Para Okta: vCenter Server 8.0 Update 1 o una versión posterior
  - Para Microsoft Entra ID: vCenter Server 8.0 Update 2 o una versión posterior
  - Para PingFederate: vCenter Server 8.0 Update 3
- Un servicio de proveedor de identidad configurado en vCenter Server
- Un proveedor de identidad externo (AD FS, Okta, Microsoft Entra ID o PingFederate)
- Una configuración de OpenID Connect (OIDC):
  - Para AD FS: un grupo de aplicaciones (también denominado aplicación)
  - Para Okta, Microsoft Entra ID o PingFederate: una aplicación de OpenID Connect
- Una aplicación del Sistema para la administración de identidades entre dominios (SCIM) para la administración de usuarios y grupos (solo para Okta, Microsoft Entra ID o PingFederate)
- Grupos y usuarios de proveedores de identidad externos que se asignan a grupos y usuarios de vCenter Server
- VMware Identity Services habilitado en vCenter Server (solo para Okta, Microsoft Entra ID o PingFederate)
- De forma opcional, para PingFederate, el certificado SSL o la cadena de certificados del servidor PingFederate, si este certificado no fue emitido por una entidad de certificación pública y conocida. Importe el certificado de SSL de PingFederate a vCenter Server.

Interoperabilidad y advertencias de la federación de proveedores de identidad de vCenter Server

La federación de proveedores de identidad de vCenter Server puede interoperar con muchas otras funciones de VMware.

Cuando planee la estrategia de federación de proveedores de identidad de vCenter Server, considere las posibles limitaciones de interoperabilidad.

Mecanismos de autenticación

En una configuración de la federación de proveedores de identidad de vCenter Server, el proveedor de identidad externo controla los mecanismos de autenticación (contraseñas, MFA, biometría, etc.).

AD FS y compatibilidad con un único dominio de Active Directory

Al configurar la federación de proveedores de identidad de vCenter Server para AD FS, el asistente Configurar proveedor de identidad principal solicita que introduzca la información de LDAP del dominio de AD único que contiene los usuarios y los grupos a los que desea acceder vCenter Server. vCenter Server deriva el dominio de AD que se utilizará para la autorización y los permisos del DN base de usuarios que especifique en el asistente. Puede agregar permisos en los objetos de vSphere solo para usuarios y grupos de este dominio de AD. Los usuarios o los grupos de dominios secundarios de AD u otros dominios del bosque de AD no son compatibles con la federación de proveedores de identidad de vCenter Server.

Compatibilidad con Okta, Microsoft Entra ID y PingFederate para varios dominios

Al configurar la federación de proveedores de identidad de vCenter Server para Okta, Microsoft Entra ID o PingFederate, el asistente Configurar proveedor de identidad principal solicita que introduzca la información de LDAP de múltiples dominios que contienen los usuarios y los grupos a los que desea acceder vCenter Server.

Directivas de contraseñas, bloqueos y tokens

Cuando vCenter Server actúa como proveedor de identidad, se controlan las directivas contraseñas, bloqueos y tokens de vCenter Server para el dominio predeterminado (vsphere.local o el nombre de dominio que introdujo al instalar vSphere). Cuando se utiliza la autenticación federada con vCenter Server, el proveedor de identidad externo controla las directivas de contraseñas, bloqueo y token para las cuentas almacenadas en el origen de identidad, como Active Directory.

Auditoría y conformidad

Cuando se utiliza la federación de proveedores de identidad de vCenter Server, vCenter Server continúa creando entradas de registro para inicios de sesión de usuarios correctos. Sin embargo, el proveedor de identidad externo es responsable de realizar un seguimiento de las acciones de registro, como los bloqueos de cuentas de usuario y los intentos de entrada de contraseña

fallidos. vCenter Server no registra estos eventos porque ya no están visibles para vCenter Server. Por ejemplo, cuando AD FS es el proveedor de identidad, realiza un seguimiento de los errores de inicios de sesión federados y los registra. Cuando vCenter Server es el proveedor de identidad para los inicios de sesión locales, vCenter Server realiza un seguimiento de los errores y los registra para los inicios de sesión locales. En una configuración federada, vCenter Server continúa registrando las acciones del usuario después del inicio de sesión.

Integración de productos VMware existentes con proveedores de identidad externos

Los productos de VMware integrados con vCenter Server (por ejemplo, VMware Aria Operations, vSAN, NSX, etc.) siguen funcionando como antes.

Productos que se integran después del inicio de sesión

Los productos que se integran después del inicio de sesión (es decir, que no requieren un inicio de sesión independiente) continúan funcionando como antes.

Autenticación simple para el acceso a API, SDK y CLI

Los scripts, los productos y otras funcionalidades existentes que se basan en los comandos de API, SDK o CLI que utilizan autenticación simple (es decir, nombre de usuario y contraseña) continúan funcionando como antes. Internamente, la autenticación se realiza pasando el nombre de usuario y la contraseña. Este paso del nombre de usuario y de la contraseña compromete algunas de las ventajas de utilizar la federación de identidades, ya que expone la contraseña a vCenter Server (y sus scripts). Considere la posibilidad de migrar a la autenticación basada en tokens siempre que sea posible.

Acceder a la interfaz de administración de vCenter Server

Si el usuario es miembro del grupo de administradores de vCenter Server, se admite el acceso a la interfaz de administración de vCenter Server (anteriormente denominada "interfaz de administración del dispositivo de vCenter Server" o VAMI).

Introducir texto de nombre de usuario en la página de inicio de sesión de AD FS

La página de inicio de sesión de AD FS no admite el envío de texto para rellenar previamente el cuadro de texto de nombre de usuario. Por ello, durante los inicios de sesión federados con AD FS, después de que introduzca el nombre de usuario en la página de destino de vCenter Server y de que se le redirija a la página de inicio de sesión de AD FS, debe volver a introducir el nombre de usuario en la página de inicio de sesión de AD FS. El nombre de usuario que introduzca en la página de destino de vCenter Server es necesario para redirigir el inicio de sesión al proveedor de identidad adecuado. Asimismo, el nombre de usuario en la página de inicio de sesión de AD FS es necesario para autenticarse con AD FS. La imposibilidad de transferir el nombre de usuario a la página de inicio de sesión de AD FS es una limitación de AD FS. No puede configurar ni cambiar este comportamiento directamente desde vCenter Server.

Compatibilidad con direcciones IPv6

AD FS, Microsoft Entra ID y Ping Federate admiten direcciones IPv6. Okta no admite direcciones IPv6.

Configuración de instancia única de VMware Identity Services

De forma predeterminada, cuando instala o actualiza a vSphere 8.0 Update 1 o posterior, la instancia de VMware Identity Services se habilita en vCenter Server. Cuando establezca Okta, Microsoft Entra ID o PingFederate en una configuración de Enhanced Link Mode, utilice VMware Identity Services en un único sistema de vCenter Server. Por ejemplo, si usa Okta en una configuración de Enhanced Mode Link que consta de tres sistemas de vCenter Server, solo se utiliza una instancia de vCenter Server de VMware Identity Services para comunicarse con el servidor de Okta.

Advertencia En una configuración de ELM que utiliza VMware Identity Services, si el sistema de vCenter Server que se comunica con el proveedor de identidad externo deja de estar disponible, puede configurar VMware Identity Services en otro vCenter Server de la configuración de ELM para interactuar con el servidor IDP externo. Consulte Proceso de activación para proveedores de identidad externos en configuraciones de Enhanced Linked Mode.

Reconfigurar el identificador de red principal

Para volver a configurar el identificador de red principal (Primary Network Identifier, PNID) del vCenter Server, es necesario actualizar la configuración del proveedor de identidad externo de la siguiente manera.

- AD FS: agregue los nuevos URI de redireccionamiento al servidor de AD FS.
- Okta: vuelva a configurar Okta. Consulte Configurar la federación de proveedores de identidad de vCenter Server para Okta y siga los pasos para crear el proveedor de identidad en vCenter Server.
- Microsoft Entra ID: reconfigurar Entra ID. Consulte Configurar la federación de proveedores de identidad de vCenter Server para Microsoft Entra ID y siga los pasos para crear el proveedor de identidad en vCenter Server.
- PingFederate: reconfigurar PingFederate. Consulte Configurar la federación de proveedores de identidad de vCenter Server para PingFederate y siga los pasos para crear el proveedor de identidad en vCenter Server.

Ciclo de vida de la federación de proveedores de identidad de vCenter Server

Al administrar el ciclo de vida de la federación de proveedores de identidad de vCenter Server, hay algunas consideraciones específicas.

Puede administrar el ciclo de vida de la federación de proveedores de identidad de vCenter Server de las siguientes maneras.

Migrar de Active Directory a un proveedor de identidad externo

Si utiliza Active Directory como origen de identidad para vCenter Server, la migración a un proveedor de identidad externo es sencilla. Si las funciones y los grupos de Active Directory coinciden con las funciones y los grupos de proveedor de identidad, no es necesario realizar ninguna acción adicional. Cuando los grupos y las funciones no coinciden, debe realizar algunos trabajos adicionales. Si vCenter Server es un miembro del dominio, considere quitarlo del dominio, ya que no es necesario ni se utiliza para la federación de identidades.

Redireccionar y migrar entre dominios

La federación de proveedores de identidad de vCenter Server admite el redireccionamiento entre dominios, es decir, el movimiento de una instancia de vCenter Server de un dominio SSO de vSphere a otro. La instancia de vCenter Server redireccionada recibe la configuración de proveedor de identidad replicada del sistema, o los sistemas, de vCenter Server a los que se ha señalado.

En general, no es necesario realizar ninguna reconfiguración adicional de proveedor de identidad para un redireccionamiento entre dominios, a menos que se cumpla una de las siguientes condiciones.

1 La configuración de proveedor de identidad de la instancia de vCenter Server redireccionada difiere de la configuración de proveedor de identidad de la instancia de vCenter Server a la que se ha señalado.

2 Esta es la primera vez que la instancia de vCenter Server redireccionada recibe una configuración de proveedor de identidad.

En estos casos, se requiere algo de trabajo adicional. Por ejemplo, para AD FS, debe agregar los URI de redireccionamiento del sistema de vCenter Server al grupo de aplicaciones correspondiente en el servidor de AD FS. Por ejemplo, si la instancia de vCenter Server 1 con el grupo de aplicaciones de AD FS A (o ninguna configuración de AD FS) se redirecciona a la instancia de vCenter Server 2 con el grupo de aplicaciones de AD FS B, debe agregar los URI de redireccionamiento de la instancia de vCenter Server 1 al grupo de aplicaciones B.

Sincronización de usuarios y grupos/copia de seguridad y restauración de vCenter Server

En función de cuándo sincronice los usuarios y grupos con vCenter Server y de cuándo realice una copia de seguridad de vCenter Server, si debe restaurar vCenter Server, es posible que deba volver a sincronizar los usuarios y grupos que SCIM insertó.

Para restaurar un usuario o un grupo eliminado, no puede simplemente insertar el usuario o el grupo desde el proveedor de identidad externo en vCenter Server. Debe actualizar la aplicación SCIM 2.0 en el proveedor de identidad externo con el usuario o el grupo faltante. Consulte Restaurar usuarios y grupos de SCIM eliminados.

Federación de proveedores de identidad de vCenter Server y Enhanced Linked Mode

Cuando se habilita la federación de proveedores de identidad en entornos de vCenter Server mediante Enhanced Linked Mode, la autenticación y los flujos de trabajo continúan funcionando como antes.

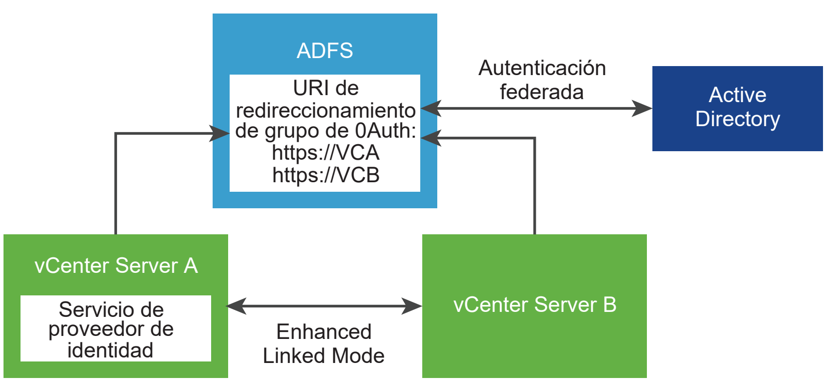
Si utiliza la configuración de Enhanced Linked Mode, tenga en cuenta lo siguiente al iniciar sesión en vCenter Server mediante la autenticación federada.

- Los usuarios siguen viendo el mismo inventario y pueden realizar las mismas acciones, según el modelo de permisos y funciones de vCenter Server.
- No es necesario que los hosts vCenter Server en Enhanced Linked Mode tengan acceso a los proveedores de identidad de los demás. Por ejemplo, considere dos sistemas vCenter Server A y B, y que utilicen Enhanced Linked Mode. Después de que vCenter Server A autoriza a un usuario, entonces, el usuario también queda autorizado en vCenter Server B.

Enhanced Link Mode y AD FS

En la siguiente figura se muestra el flujo de trabajo de autenticación cuando se utiliza AD FS con Enhanced Linked Mode.

Figura 4-4. La federación de proveedores de identidad de AD FS y Enhanced Linked Mode



1. Se implementan dos nodos de vCenter Server en la configuración de Enhanced Linked Mode.
2. La configuración de AD FS se estableció en vCenter Server A mediante el asistente Cambiar proveedor de identidad en vSphere Client. También se establecieron membresías a grupos y permisos para ellos para los usuarios o grupos de AD FS.
3. vCenter Server A replica la configuración de AD FS en vCenter Server B.
4. Todos los URI de redirección de los dos nodos de vCenter Server se agregan al grupo de aplicaciones OAuth en AD FS. Solo se crea un grupo de aplicaciones OAuth.
5. Cuando un usuario inicia sesión y está autorizado por vCenter Server A, también se autoriza el usuario en vCenter Server B. Si el usuario inicia sesión primero en vCenter Server B, sucederá lo mismo.

Escenarios de configuración de Enhanced Linked Mode con AD FS

vCenter Server Enhanced Linked Mode admite los siguientes escenarios de configuración para AD FS. En esta sección, el término "configuración de AD FS" hace referencia a la configuración que se establece en vSphere Client mediante el asistente Cambiar proveedor de identidad y cualquier membresía a grupos o permisos de este que se hayan establecido para usuarios o grupos de AD FS.

Habilitar AD FS en una configuración de Enhanced Linked Mode existente

Pasos de alto nivel:

1 Implemente N nodos de vCenter Server en la configuración de Enhanced Linked Mode.

2 Configure AD FS en uno de los nodos vinculados de vCenter Server.

3 La configuración de AD FS se replica a todos los demás nodos (N-1) de vCenter Server.

4 Agregue todos los URI de redirección para la totalidad de los N nodos de vCenter Server al grupo de aplicaciones OAuth configurado en AD FS.

Vincular una nueva instancia de vCenter Server a una configuración de AD FS con Enhanced Linked Mode existente

Pasos de alto nivel:

1 (Requisito previo) Configure AD FS en un ajuste de Enhanced Linked Mode de nodo N de vCenter Server.

2 Implemente un nuevo nodo de vCenter Server independiente.

3 Redireccione la nueva instancia de vCenter Server al dominio de Enhanced Linked Mode de AD FS de nodo N mediante uno de los nodos *N* como su socio de replicación.

4 Toda la configuración de AD FS en la configuración de Enhanced Linked Mode existente se replica en la nueva instancia de vCenter Server.

  La configuración de AD FS que está en el dominio de Enhanced Linked Mode de AD FS de nodo N sobrescribe cualquier configuración existente de AD FS en la instancia de vCenter Server recién vinculada.

5 Agregue todos los URI de redirección para la nueva instancia de vCenter Server al grupo de aplicaciones OAuth configurado existente en AD FS.

Desvincular una instancia de vCenter Server de una configuración de AD FS con Enhanced Linked Mode

Pasos de alto nivel:

1 (Requisito previo) Configure AD FS en un ajuste de Enhanced Linked Mode de vCenter Server de nodo N.

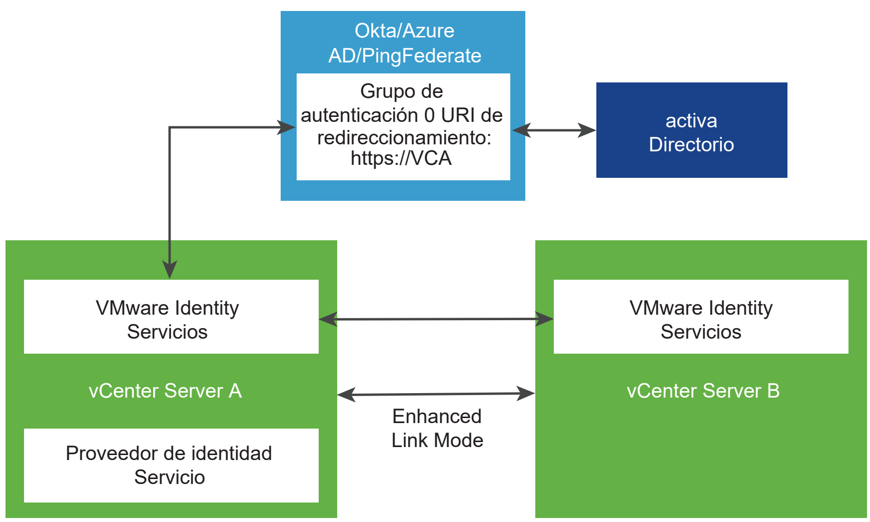
2 Elimine del registro uno de los hosts de vCenter Server en la configuración de nodo N y redirecciónelo a un nuevo dominio para desvincularlo de la configuración de nodo N.

3 El proceso de redireccionamiento de dominio no conserva la configuración de SSO, por lo que todas las opciones de AD FS del nodo de vCenter Server desvinculado se revierten y se pierden. Para continuar usando AD FS en este nodo de vCenter Server desvinculado, debe volver a configurar AD FS desde el principio o volver a vincular la instancia de vCenter Server a una configuración de Enhanced Linked Mode en la que AD FS ya esté configurado.

Enhanced Linked Mode y Okta, Microsoft Entra ID o PingFederate Identity Provider Federation

En la siguiente figura se muestra el flujo de trabajo de autenticación cuando se utiliza Okta, Microsoft Entra ID o PingFederate con Enhanced Linked Mode.

Figura 4-5. Enhanced Linked Mode y Okta, Microsoft Entra ID o PingFederate Identity Provider Federation



Nota Al configurar Okta, Microsoft Entra ID o PingFederate como proveedor de identidad externo, todos los sistemas de vCenter Server en una configuración de Enhanced Linked Mode deben ejecutar al menos vSphere 8.0 Update 1 para Okta, vSphere 8.0 Update 2 para Microsoft Entra ID y vSphere 8.0 Update 3 para PingFederate.

1 Se implementan dos nodos de vCenter Server en la configuración de Enhanced Linked Mode.

2 La configuración de Okta, Microsoft Entra ID o PingFederate se configuró en vCenter Server A mediante el asistente Cambiar proveedor de identidad en la instancia de vSphere Client. También se establecieron pertenencias a grupos y permisos para los usuarios o grupos de Okta, Microsoft Entra ID o PingFederate.

   Nota Tanto vCenter Server A como B tienen habilitados servicios de VMware Identity Services, pero solo los servicios de VMware Identity Services de vCenter Server A se comunican con el servidor del proveedor de identidad.

3 Las instancias de VMware Identity Services que se ejecutan en vCenter Server A habilitan a vCenter Server B para que acceda a su endpoint.

4 El URI de redireccionamiento de vCenter Server A se agrega a la aplicación OAuth en Okta, Microsoft Entra ID o PingFederate. Solo se crea una aplicación de OAuth.

5 Cuando un usuario inicia sesión y está autorizado por vCenter Server A, también se autoriza el usuario en vCenter Server B. Si el usuario inicia sesión primero en vCenter Server B, sucederá lo mismo.

Situaciones de configuración de Enhanced Linked Mode con Okta, ID de Microsoft Entra o PingFederate

vCenter Server Enhanced Linked Mode admite las siguientes situaciones de configuración para Okta, Microsoft Entra ID y PingFederate. En esta sección, "ajustes de Okta" y "configuración de Okta", "ajustes de Microsoft Entra ID" y "configuración de Microsoft Entra ID" o "ajustes de PingFederate" y "configuración de PingFederate" hacen referencia a los ajustes que se establecen en el vSphere Client mediante el asistente Cambiar proveedor de identidad y cualquier pertenencia a grupos o permisos de este que se hayan establecido para usuarios o grupos de Okta, Microsoft Entra ID o PingFederate.

Habilitar Okta, Microsoft Entra ID o PingFederate en una configuración de Enhanced Linked Mode existente

Pasos de alto nivel:

1 Implemente N nodos de vCenter Server en la configuración de Enhanced Linked Mode.

2 Configure Okta, Microsoft Entra ID o PingFederate en uno de los nodos de vCenter Server vinculados.

3 La información del endpoint de VMware Identity Services se replica en todos los demás nodos de vCenter Server (N-1).

   La información de configuración de Okta, Microsoft Entra ID o PingFederate (identificador de cliente compartido, etc.) y la información de usuario/grupo no se replica.

Vincular una nueva instancia de vCenter Server a una configuración existente de Okta, Microsoft Entra ID o PingFederate con Enhanced Linked Mode

Pasos de alto nivel:

1 (Requisito previo) Configure Okta, Microsoft Entra ID o PingFederate en una configuración de Enhanced Linked Mode de nodo N de vCenter Server.

2 Implemente un nuevo nodo de vCenter Server independiente.

3 Redireccione la nueva instancia de vCenter Server al dominio de Enhanced Linked Mode de Okta, Microsoft Entra ID o PingFederate de nodo N mediante uno de los nodos *N* como su socio de replicación.

4 La información del endpoint de VMware Identity Services se replica en todos los demás nodos de vCenter Server (N-1).

La información de configuración de Okta, Microsoft Entra ID o PingFederate (identificador de cliente compartido, etc.) y la información de usuario/grupo no se replica.

Nota No se puede agregar un nodo de vCenter Server con una configuración existente de VMware Identity Services. En este escenario, la configuración existente de VMware Identity Services se reemplaza por la configuración de Enhanced Link Mode de VMware Identity Services a la que se une.

No se puede agregar un nodo de vCenter Server con una configuración de VMware Identity Services existente a una configuración de ELM que no se haya configurado con VMware Identity Services. En este escenario, elimine primero del vCenter Server la configuración de VMware Identity Services existente antes de agregarla a la configuración de ELM.

Desvincular una instancia de vCenter Server de una configuración de Okta, Microsoft Entra ID o PingFederate con Enhanced Linked Mode

Pasos de alto nivel:

1 (Requisito previo) Configure Okta, Microsoft Entra ID o PingFederate en una configuración de Enhanced Linked Mode de nodo N de vCenter Server.

2 Elimine del registro uno de los hosts de vCenter Server en la configuración de nodo N y redirecciónelo a un nuevo dominio para desvincularlo de la configuración de nodo N.

3 El proceso de redireccionamiento de dominio no conserva la configuración de SSO, por lo que todas las opciones de Okta, Microsoft Entra ID o PingFederate del nodo de vCenter Server desvinculado se revierten y se pierden. Para continuar usando Okta, Microsoft Entra ID o PingFederate en este nodo de vCenter Server desvinculado, debe volver a configurar Okta, Microsoft Entra ID o PingFederate desde el principio, o bien volver a vincular la instancia de vCenter Server a una configuración de Enhanced Linked Mode en la que Okta, Microsoft Entra ID o PingFederate ya estén configurados.

Nota No se puede desvincular una instancia de vCenter Server con una configuración activa de VMware Identity Services.

Proceso de activación para proveedores de identidad externos en configuraciones de Enhanced Linked Mode

Obtenga más información sobre las consideraciones de disponibilidad en las configuraciones de Enhanced Linked Mode con Okta, Microsoft Entra ID o PingFederate.

Requisitos previos

- Dos o más sistemas de vCenter Server en una configuración de Enhanced Linked Mode. Por ejemplo, los sistemas se etiquetan como VC_1, VC_2 y VC_3, a través de VC_N, donde N es el número de sistemas de vCenter Server en la configuración de Enhanced Linked Mode.

- Para Okta y Microsoft Entra ID, todos los sistemas de vCenter Server deben ejecutar vSphere 8.0 Update 2 o versiones posteriores. Para PingFederate, todos los sistemas de vCenter Server deben ejecutar al menos vSphere 8.0 Update 3.
- Okta, Microsoft Entra ID o PingFederate están configurados como proveedores de identidad externos en uno de los sistemas de vCenter Server. Por ejemplo, la etiqueta del sistema es VC_1.
- El proveedor de identidad externo está configurado con todas las aplicaciones de OAuth2 y SCIM requeridas.

Procedimiento

1 Para activar una instancia de vCenter Server VC_i determinada, en la que i se sitúa entre 2 y N:

   a Obtenga acceso de shell local a VC_i para ejecutar el script de activación.

   Nota Para realizar los pasos siguientes, la cuenta de usuario de vCenter Server con privilegios de administrador se puede asignar en la línea de comandos o en las solicitudes de la consola.

   b Ejecute `'status'` desde el script de activación para obtener el estado de activación actual de vCenter Server.

   ```
   python /usr/lib/vmware-trustmanagement/vmware_identity_services_activation.py status
   ```

   c Si el comando `'status'` indica que vCenter Server no está activado, ejecute `'activate'` en el script de activación:

   ```
   python /usr/lib/vmware-trustmanagement/vmware_identity_services_activation.py activate
   ```

   d Si el comando `'status'` indica que vCenter Server ya está activado, ejecute la opción `'deactivate'` y, a continuación, la opción `'activate'`.

   ```
   python /usr/lib/vmware-trustmanagement/vmware_identity_services_activation.py
   deactivate
   ```

   - Por ejemplo, ejecute la opción `'activate'`.
   - Si lo prefiere, puede especificar la opción `'--force-replace'` en el comando `'activate'`.

2 Abra un navegador en vCenter Server VC_i e inicie sesión como administrador en vCenter Server.

   a Desplácese hasta **Inicio > Administración > Inicio de sesión único > Configuración**.

   b En **Aprovisionamiento de usuarios**, compruebe que **URL de tenant** contenga el FQDN de VC_i.

c Copie la cadena de **URL de tenant** y guarde esta información para utilizarla con el proveedor de identidad externo.

d En **Token secreto**, haga clic en **Generar**, copie la cadena de token generada y guarde esta información para usarla con el proveedor de identidad externo.

e En **OpenID Connect**, compruebe que **URI de redireccionamiento** contenga el FQDN de VC_i.

f Copie la cadena de **URI de redireccionamiento** y guarde esta información para utilizarla con el proveedor de identidad externo.

3 Abra un navegador en la página de administración del proveedor de identidad externo.

Nota Para obtener más información, consulte los detalles específicos del proveedor de identidad externo para llevar a cabo los siguientes pasos.

---

a Busque el registro de OAuth2 que se configuró cuando el proveedor de identidad externo estaba configurado originalmente en VC_1.

b Edite el registro de OAuth2 y agregue el URI de redireccionamiento que se obtuvo anteriormente para VC_i.

c Si el proveedor de identidad externo admite configuraciones push de SCIM con varios destinos:

- Busque la configuración push de SCIM que se estableció cuando el proveedor de identidad externo estaba originalmente configurado en VC_1.
- Edite la configuración push de SCIM y agregue los valores de **URL de tenant** y **Token secreto** que se obtuvieron previamente para VC_i.

d Si el proveedor de identidad externo admite configuraciones push de SCIM con un solo destino:

- Cree una configuración push de SCIM nueva con los valores de **URL de tenant** y **Token secreto** que se obtuvieron anteriormente para VC_i.
- Asegúrese de que la configuración push de SCIM esté insertando los mismos datos de usuario o grupo que la configuración push de SCIM que se estableció cuando el proveedor de identidad externo estaba originalmente configurado en VC_1.

e Inicie una operación push de SCIM para asegurarse de que VC_i se rellene con los datos de usuario o grupo más recientes.

Configurar la federación de proveedores de identidad de vCenter Server

Después de implementar vCenter Server inicialmente, puede configurar un proveedor de identidad externo para la autenticación federada.

vSphere 7.0 y versiones posteriores son compatibles con Active Directory Federation Services (AD FS). Solo vSphere 8.0 Update 1 y versiones posteriores son compatibles con Okta. vSphere 8.0 Update 2 y versiones posteriores admiten Microsoft Entra ID (anteriormente denominado Azure AD). A partir de vSphere 8.0 Update 3, vSphere admite PingFederate.

Configure la federación de proveedores de identidad de vCenter Server desde la instancia de vSphere Client o la API. También debe realizar algunas tareas de configuración en el proveedor de identidad externo. Para configurar la federación de proveedores de identidad de vCenter Server, se deben tener privilegios de administrador de vCenter Single Sign-On. Tener privilegios de administrador de vCenter Single Sign-On es diferente a tener función de administrador en vCenter Server o ESXi. En una nueva instalación, solo el administrador de vCenter Single Sign-On (administrator@vsphere.local de forma predeterminada) puede autenticarse en vCenter Single Sign-On.

Flujo del proceso de configuración de la federación de proveedores de identidad de vCenter Server

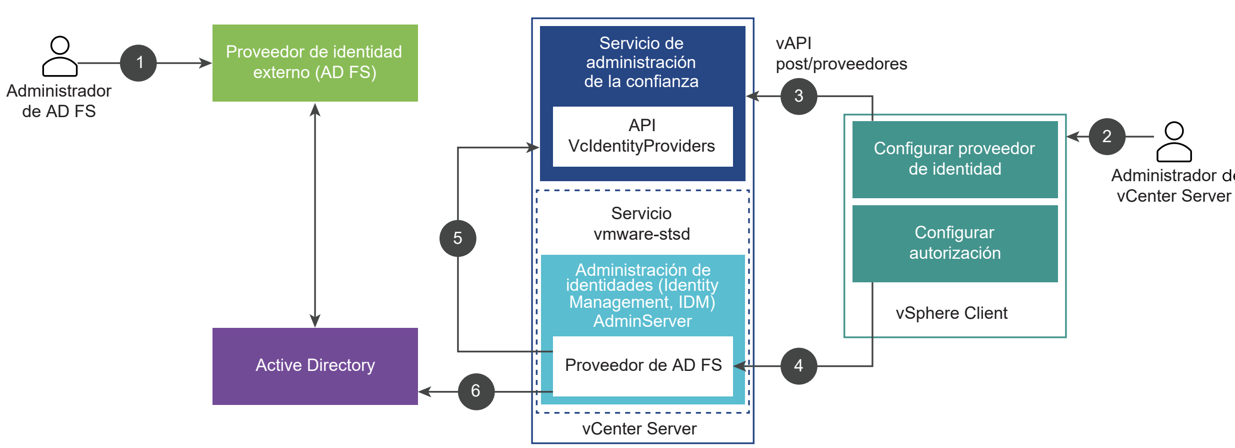
Para configurar eficazmente la federación de proveedores de identidad de vCenter Server, debe comprender los flujos de comunicación que se producen.

Puede configurar la federación de proveedores de identidad de vCenter Server para AD FS, Microsoft Entra ID (anteriormente Azure AD), Okta o PingFederate.

Flujo del proceso de configuración de la federación de proveedores de identidad de vCenter Server para AD FS

En la siguiente figura, se muestra el flujo del proceso que se produce al configurar la federación de proveedores de identidad de vCenter Server para AD FS.

Figura 4-6. Flujo del proceso de configuración de la federación de proveedores de identidad de vCenter Server para AD FS



vCenter Server, AD FS y Active Directory interactúan de la siguiente manera.

1 El administrador de AD FS configura una aplicación OIDC de AD FS para vCenter Server.

2 El administrador de vCenter Server inicia sesión en vCenter Server mediante vSphere Client.

3 El administrador de vCenter Server agrega un proveedor de identidad de AD FS a vCenter Server y también introduce información sobre el dominio de Active Directory.

   vCenter Server necesita esta información para hacer una conexión LDAP con el dominio de Active Directory del servidor de AD FS. Con esta conexión, vCenter Server busca usuarios y grupos y los agrega a grupos locales de vCenter Server en el siguiente paso. Consulte la sección titulada "Buscar en el dominio de Active Directory" que se incluye a continuación para obtener más información.

4 El administrador de vCenter Server configura los permisos de autorización en vCenter Server para los usuarios de AD FS.

5 El proveedor de AD FS consulta a la API de VcIdentityProviders para obtener la información de la conexión LDAP para el origen de Active Directory.

6 El proveedor de AD FS busca en Active Directory los grupos o usuarios consultados para finalizar la configuración de la autorización.

Buscar en el dominio de Active Directory

Para configurar AD FS como el proveedor de identidad externo en vCenter Server, puede usar el asistente Configurar proveedor de identidad principal en vSphere Client. Como parte del proceso de configuración, debe introducir información sobre el dominio de Active Directory, incluida la información del nombre distintivo del usuario y el grupo. Para configurar AD FS para la autenticación, se necesita esta información de conexión de Active Directory. Esta conexión es necesaria para buscar y asignar nombres de usuarios y grupos de Active Directory a funciones y permisos en vCenter Server, mientras que AD FS se utiliza para la autenticación del usuario. Este paso del asistente Configurar proveedor de identidad principal no crea un origen de identidad de Active Directory en LDAP. En lugar de ello, vCenter Server utiliza esta información para establecer una conexión válida apta para búsqueda en el dominio de Active Directory para buscar usuarios y grupos allí.

Considere un ejemplo usando las siguientes entradas de nombre distintivo:

- Nombre distintivo base para usuarios: cn=Users,dc=corp,dc=local
- Nombre distintivo base para grupos: dc=corp,dc=local
- Nombre de usuario: cn=Administrator,cn=Users,dc=corp,dc=local

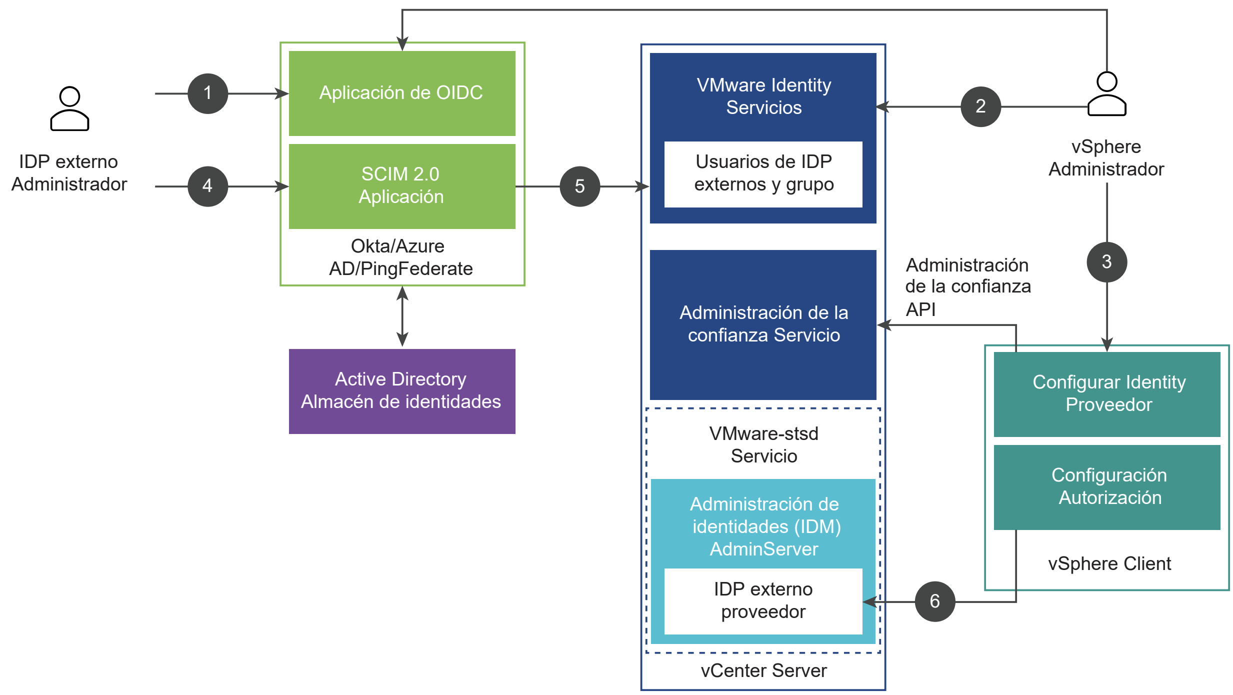
Si el usuario AdfsUser@corp.local es miembro del grupo ADGroup@corp.local, la introducción de esta información en el asistente permite que un administrador de vCenter Server busque y encuentre el grupo ADGroup@corp.local, y lo agregue al grupo Administrators@vsphere.local de vCenter Server. Como resultado, el usuario AdfsUser@corp.local recibe privilegios administrativos en vCenter Server al iniciar sesión.

vCenter Server también utiliza este proceso de búsqueda cuando se configuran permisos globales para usuarios y grupos de Active Directory. En ambos casos, ya sea al configurar permisos globales o agregar un usuario o grupo, seleccione el dominio que ha introducido para su proveedor de identificación AD FS en el menú desplegable **Dominio** para buscar y seleccionar usuarios y grupos del dominio de Active Directory.

Flujo del proceso de configuración de la federación de proveedores de identidad de vCenter Server mediante VMware Identity Services

Para configurar Okta, Microsoft Entra ID y PingFederate, utilice VMware Identity Services. En la siguiente figura se muestra el flujo del proceso que se produce al configurar la federación de proveedores de identidad de vCenter Server para VMware Identity Services.

Figura 4-7. Flujo del proceso de configuración de la federación de proveedores de identidad de vCenter Server mediante VMware Identity Services



vCenter Server, VMware Identity Services y Active Directory interactúan de la siguiente manera.

1 El administrador de IDP externo configura una aplicación OIDC para vCenter Server.

2 El administrador de vCenter Server inicia sesión en vCenter Server mediante vSphere Client, agrega un proveedor de identidad a vCenter Server y también introduce la información del dominio.

3 El administrador de vCenter Server proporciona el URI de redireccionamiento (obtenido de la página de configuración del proveedor de identidad en vSphere Client) al administrador del proveedor de identidad para agregarlo a la aplicación OIDC creada en el paso 2.

4 El administrador de IDP externo configura una aplicación SCIM 2.0.

5 El administrador de IDP externo asigna los usuarios y grupos a la aplicación SCIM 2.0 e inserta los usuarios y grupos en vCenter Server.

6 El administrador de vCenter Server configura los permisos de autorización en vCenter Server para los usuarios de IDP externos.

Usuarios y grupos de IDP externos

Puesto que un proveedor de identidad externo usa el sistema para la administración de identidades entre dominios (SCIM) para usuarios y grupos, dichos usuarios y grupos residen en la instancia de vCenter Server. Al buscar usuarios y grupos en el proveedor de identidad externo, por ejemplo para asignar permisos, la búsqueda se realiza de forma local en el vCenter Server.

vCenter Server también utiliza este proceso de búsqueda cuando se configuran permisos globales para usuarios y grupos de IDP externos. En ambos casos, ya sea al configurar permisos globales o agregar un usuario o grupo, seleccione el dominio que haya introducido para su proveedor de identidad desde el menú desplegable **Dominio** a fin de buscar y seleccionar usuarios y grupos desde el dominio.

Usar el almacén de certificados raíz de confianza en lugar del almacén de confianza de JRE

Si importó un certificado de CA raíz emitido por su propia entidad de certificación interna al almacén de confianza de JRE en vSphere 7.0, a partir de vSphere 7.0 Update 1, puede registrar el certificado en el almacén de certificados raíz de confianza.

Para configurar la federación de proveedores de identidad de vCenter Server en vSphere 7.0 con un certificado de CA raíz emitido por su propia entidad de certificación interna, debe haberlo importarlo al almacén de confianza de JRE. A partir de vSphere 7.0 Update 1, puede registrar el certificado en el almacén de certificados raíz de confianza. Este cambio significa que debe agregar el certificado de CA raíz emitido por su propia entidad de certificación interna al almacén de certificados raíz de confianza (también denominado VMware Endpoint Certificate Store o VECS). Los certificados en el almacén de confianza de JRE continúan funcionando; sin embargo, vCenter Server está normalizando el uso del almacén de certificados raíz de confianza.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

   Nota Para obtener más información, consulte Agregar un certificado raíz de confianza al almacén de certificados mediante vSphere Client.

2 Desplácese hasta **Administración > Certificados > Administración de certificados**.

3 Junto a **Certificados raíz de confianza**, haga clic en **Agregar**.

4 Busque el certificado raíz de AD FS y haga clic en **Agregar**.

   El certificado se agrega a un panel bajo **Certificados raíz de confianza**.

Configurar la federación de proveedores de identidad de vCenter Server para AD FS

Después de instalar o actualizar a vSphere 7.0 o una versión posterior, puede configurar la federación de proveedores de identidad de vCenter Server para AD FS como un proveedor de identidad externo.

Nota Estas instrucciones son para vSphere 8.0 Update 1 y versiones posteriores. Para vSphere 8.0, consulte el tema sobre cómo configurar la federación de proveedores de identidad de vCenter Server para AD FS en la documentación de *vSphere Authentication* en https://docs.vmware.com/es/VMware-vSphere/8.0/vsphere-documentation-80.zip.

vCenter Server admite solo un proveedor de identidad externo configurado y el origen de identidad vsphere.local. No se pueden utilizar varios proveedores de identidad externos. La federación de proveedores de identidad de vCenter Server usa OpenID Connect (OIDC) para los inicios de sesión del usuario en vCenter Server.

En esta tarea se describe cómo agregar un grupo de AD FS al grupo Administradores de vSphere como forma de controlar los permisos. También puede configurar los privilegios mediante la autorización de AD FS a través de permisos globales o de objeto en vCenter Server. Consulte la documentación de *Seguridad de vSphere* para obtener más información sobre cómo agregar permisos.

Precaución Si utiliza un origen de identidad de Active Directory ya agregado previamente a vCenter Server como el origen de identidad de AD FS, no elimine ese origen de identidad de vCenter Server. Si lo hace, se produce una regresión de las funciones y pertenencias a grupos asignadas previamente. Tanto el usuario de AD FS con permisos globales como los usuarios que se agregaron al grupo Administradores no podrán iniciar sesión.

Solución alternativa: si no necesita las funciones y pertenencias a grupos asignadas previamente y desea eliminar el origen de identidad de Active Directory anterior, elimine el origen de identidad antes de crear el proveedor de AD FS y configurar las pertenencias a grupos en vCenter Server.

Requisitos previos

Nota Este proceso de configuración de un proveedor de identidad de AD FS requiere que tenga acceso administrativo tanto al servidor de vCenter Server como al servidor de AD FS. Durante el proceso de configuración, primero debe introducir la información en vCenter Server y en el servidor de AD FS y, a continuación, en vCenter Server.

Requisitos de los servicios de Federación de Active Directory:

- AD FS para Windows Server 2016 o una versión posterior debe estar ya implementado.
- AD FS debe estar conectado a Active Directory.

- Como parte del proceso de configuración, se debe crear un grupo de aplicaciones de vCenter Server en AD FS. Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/78029.
- Un certificado de servidor de AD FS (o una CA o un certificado intermedio que firmó el certificado del servidor de AD FS) que se agrega al almacén de certificados raíz de confianza.
- Ha creado un grupo de administradores de vCenter Server en AD FS que contiene los usuarios a los que desea conceder privilegios de administrador de vCenter Server.

Para obtener más información sobre cómo configurar AD FS, consulte la documentación de Microsoft.

Requisitos de vCenter Server y otros:

- vSphere 7.0 o posterior
- vCenter Server debe poder conectarse al endpoint de detección de AD FS y a los endpoint de autorización, token, cierre de sesión, JWKS y de cualquier otra índole que estén anunciado en los metadatos de endpoint de detección.
- Se necesita el privilegio **VcIdentityProviders.Administrar** para crear, actualizar o eliminar un proveedor de identidad de vCenter Server que es necesario para la autenticación federada. Para limitar un usuario de forma que solamente pueda ver la información de configuración del proveedor de identidad, asigne el privilegio **VcIdentityProviders.Leer**.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Agregue el certificado del servidor de AD FS (o una CA o un certificado intermedio que firmó el certificado del servidor de AD FS) al almacén de certificados raíz de confianza.

Nota Para obtener más información, consulte Agregar un certificado raíz de confianza al almacén de certificados mediante vSphere Client.

a Desplácese hasta **Administración > Certificados > Administración de certificados**.

b Junto al **almacén raíz de confianza**, haga clic en **Agregar**.

c Busque el certificado de AD FS y haga clic en **Agregar**.

El certificado se agrega a un panel bajo **Certificados raíz de confianza**.

3 Comience a crear el proveedor de identidad en vCenter Server.

a Utilice vSphere Client para iniciar sesión como administrador en vCenter Server.

b Desplácese hasta **Inicio > Administración > Inicio de sesión único > Configuración**.

c Haga clic en **Proveedor de cambio** y seleccione **ADFS**.

Se abrirá el asistente **Configurar proveedor de identidad principal**.

d En el panel **Requisitos previos**, revise los requisitos de AD FS y vCenter Server.

e Haga clic en **Ejecutar comprobaciones previas**.

Si la comprobación previa encuentra errores, haga clic en **Ver detalles** y siga los pasos para resolver los errores como se indica.

f Cuando se apruebe la comprobación previa, haga clic en la casilla de confirmación y, a continuación, haga clic en **Siguiente**.

g En el panel **Usuarios y grupos**, introduzca la información de usuario y de grupo de la conexión de Active Directory en LDAP para buscar usuarios y grupos.

vCenter Server toma el dominio de AD que se utilizará para la autorización y los permisos del nombre distintivo base para los usuarios. Puede agregar permisos en los objetos de vSphere solo para usuarios y grupos de este dominio de AD. Los usuarios o los grupos de dominios secundarios de AD u otros dominios del bosque de AD no son compatibles con la federación de proveedores de identidad de vCenter Server.

Opción	Descripción
Nombre distintivo base para usuarios	El nombre distinguido base para los usuarios.
Nombre distintivo base para grupos	El nombre distinguido base para grupos.
Nombre de usuario	Identificador de un usuario del dominio que tiene, como mínimo, acceso de solo lectura al DN base para los usuarios y los grupos.
Contraseña	Identificador de un usuario del dominio que tiene, como mínimo, acceso de solo lectura al DN base para los usuarios y los grupos.
URL de servidor principal	El servidor LDAP de la controladora de dominio principal para el dominio. Use el formato `ldap://nombre de host:puerto` o `ldaps://nombre de host:puerto`. Por lo general, el puerto es el 389 para las conexiones de LDAP y 636 para las conexiones de LDAPS. Para las implementaciones de controladoras de varios dominios de Active Directory, el puerto suele ser el 3268 para las conexiones de LDAP y el 3269 para las conexiones de LDAPS. Se necesita un certificado que establezca la confianza para el endpoint de LDAPS del servidor Active Directory cuando se usa `ldaps://` en la dirección URL del servidor LDAP principal o secundario.
URL de servidor secundario	Dirección de un servidor LDAP de controladora de dominio secundario que se usa para la conmutación por error.
certificados SSL	Si desea utilizar LDAPS con el servidor de LDAP de Active Directory o el origen de identidad del servidor OpenLDAP, haga clic en `Examinar` para seleccionar un certificado.

h Haga clic en **Siguiente**.

i En el panel **OpenID Connect**, copie el URI de redireccionamiento y el URI de redireccionamiento de cierre de sesión.

Deje los otros campos en blanco por ahora. Vuelva al panel **OpenID Connect** después de crear la configuración de conexión de OpenID en el siguiente paso.

4 Cree una configuración de OpenID Connect en AD FS y configúrela para vCenter Server.

Para establecer una relación de confianza para usuario autenticado entre vCenter Server y un proveedor de identidad, debe establecer la información de identificación y un secreto compartido entre ellos. Para llevar esto a cabo en AD FS, debe crear una configuración de OpenID Connect, conocida como grupo de aplicaciones, que consta de una aplicación de servidor y una API web. Los dos componentes especifican la información que vCenter Server usa para confiar en el servidor de AD FS y comunicarse con él. Para habilitar OpenID Connect en AD FS, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/78029.

Tenga en cuenta lo siguiente al crear el grupo de aplicaciones de AD FS.

- Necesita los dos URI de redireccionamiento de vCenter Server obtenidos en el paso anterior.
- Copie la siguiente información del grupo de aplicaciones de AD FS en un archivo o anótela para usarla cuando finalice la creación del proveedor de identidad de vCenter Server en el siguiente paso.
  - Identificador de cliente
  - Secreto compartido
  - Dirección de OpenID del servidor de AD FS

Nota Si es necesario, obtenga la dirección de OpenID del servidor de AD FS ejecutando el siguiente comando de PowerShell como administrador de AD FS.

```
Get-AdfsEndpoint | Select FullUrl | Select-String openid-configuration
```

Copie la URL que se devuelve (seleccione solo la URL en sí, no el paréntesis de cierre ni la parte `"@{FullUrl="` inicial).

---

5 En el panel vCenter Server **OpenID Connect**:

a Introduzca la siguiente información que obtuvo en el paso anterior al crear el grupo de aplicaciones de AD FS:

- Identificador de cliente
- Secreto compartido
- Dirección de OpenID

El nombre del proveedor de identidad se rellena automáticamente como Microsoft ADFS.

b Haga clic en **Siguiente**.

6 Revise la información y haga clic en **Finalizar**.

vCenter Server crea el proveedor de identidad de AD FS y muestra la información de configuración.

7 Configure la pertenencia a grupos en vCenter Server para la autorización de AD FS.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

   c Haga clic en la pestaña **Grupos**.

   d Haga clic en el grupo **Administradores** y, a continuación, en **Agregar miembros**.

   e Seleccione el dominio en el menú desplegable.

   f En el cuadro de texto que se encuentra debajo del menú desplegable, introduzca los primeros caracteres del grupo de AD FS que desea agregar y, a continuación, espere a que aparezca la selección desplegable.

      Es posible que esta selección tarde varios segundos en aparecer, ya que vCenter Server establece la conexión con Active Directory y busca en él.

   g Seleccione el grupo de AD FS y añádalo al grupo Administradores.

   h Haga clic en **Guardar**.

8 Confirme que se puede iniciar sesión en vCenter Server con un usuario de Active Directory.

Configurar la federación de proveedores de identidad de vCenter Server para Okta

Después de instalar o actualizar a vSphere 8.0 Update 1 o una versión posterior, puede configurar la federación de proveedores de identidad de vCenter Server para Okta como proveedor de identidad externo.

vCenter Server admite solo un proveedor de identidad externo configurado y el origen de identidad vsphere.local (fuente local). No se pueden utilizar varios proveedores de identidad externos. La federación de proveedores de identidad de vCenter Server usa OpenID Connect (OIDC) para los inicios de sesión del usuario en vCenter Server.

Puede configurar privilegios mediante usuarios y grupos de Okta a través de permisos globales o de objetos en vCenter Server. Consulte la documentación de *Seguridad de vSphere* para obtener más información sobre cómo agregar permisos.

Requisitos previos

Requisitos de Okta:

- Es cliente de Okta y tiene un espacio de dominio, por ejemplo, https://*your-company*.okta.com.
- Para realizar inicios de sesión en OIDC y administrar permisos de usuario y grupo, debe crear las siguientes aplicaciones de Okta.
  - Una aplicación nativa de Okta con OpenID Connect como método de inicio de sesión. La aplicación nativa debe incluir los tipos de concesión de código de autorización, token de actualización y contraseña del propietario del recurso.

  - Una aplicación de Sistema para la administración de identidades entre dominios (SCIM) 2.0 con un token de portador OAuth 2.0 para realizar la sincronización de usuarios y grupos entre el servidor de Okta y vCenter Server.

  Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/90835.

- Identificó los usuarios y grupos de Okta que desea compartir con vCenter Server. Este uso compartido es una operación SCIM (no una operación OIDC).

Requisitos de conectividad de Okta:

- vCenter Server debe poder conectarse al endpoint de detección de Okta y a los endpoint de autorización, token, JWKS y de cualquier otra índole que estén anunciado en los metadatos de endpoint de detección.
- Okta también debe poder conectarse con vCenter Server para enviar datos de usuarios y grupos para el aprovisionamiento de SCIM.

Requisitos de vCenter Server:

- vSphere 8.0 Update 1 o una versión posterior
- En vCenter Server donde desea crear el origen de identidad de Okta, compruebe que VMware Identity Services esté activado.

  Nota Al instalar o actualizar a vSphere 8.0 Update 1 o una versión posterior, los servidores de identidad de VMware se activan de forma predeterminada. Puede utilizar la interfaz de administración de vCenter Server para confirmar el estado de VMware Identity Services. Consulte Detener e iniciar VMware Identity Services.

Requisitos de privilegios de vSphere:

- Debe tener el privilegio **VcIdentityProviders.Administrar** para crear, actualizar o eliminar un proveedor de identidad de vCenter Server que es necesario para la autenticación federada. Para limitar un usuario de forma que solamente pueda ver la información de configuración del proveedor de identidad, asigne el privilegio **VcIdentityProviders.Leer**.

Requisitos de Enhanced Linked Mode:

- Puede configurar la federación de proveedores de identidad de vCenter Server para Okta en una configuración de Enhanced Linked Mode. Cuando configure Okta en Enhanced Link Mode, se configura el proveedor de identidad de Okta para que utilice VMware Identity Services en un único sistema vCenter Server. Por ejemplo, si la configuración de Enhanced Mode Link consta de dos sistemas vCenter Server, solo se utilizará una instancia de vCenter Server y su instancia de VMware Identity Services para comunicarse con el servidor Okta. Si este sistema vCenter Server deja de estar disponible, puede configurar VMware Identity Services en otra instancia de vCenter Server de la configuración de ELM para interactuar con el servidor de Okta. Para obtener más información, consulte Proceso de activación para proveedores de identidad externos en configuraciones de Enhanced Linked Mode.

- Al configurar Okta como proveedor de identidad externo, todos los sistemas vCenter Server en una configuración de Enhanced Linked Mode deben ejecutar al menos vSphere 8.0 Update 1.

Requisitos de red:

- Si la red no es de acceso público, debe crear un túnel de red entre el sistema vCenter Server y el servidor Okta y, a continuación, utilizar la URL de acceso público adecuada como URI base.

Procedimiento

1. Cree una aplicación de OpenID Connect en Okta y asigne grupos y usuarios a la aplicación OpenID Connect.

   Para crear la aplicación OpenID Connect y asignar grupos y usuarios, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/90835. Siga los pasos de la sección titulada "Crear la aplicación OpenID Connect". Después de crear la aplicación Okta OpenID Connect, copie la siguiente información de la aplicación en un archivo para usarlo al configurar el proveedor de identidad de vCenter Server en el siguiente paso.

   - Identificador de cliente
   - Secreto de cliente (que se muestra como secreto compartido en vSphere Client)
   - Información de dominio de Active Directory o información de dominio de Okta si no está ejecutando Active Directory

2. Para crear el proveedor de identidad en vCenter Server:

   a. Utilice vSphere Client para iniciar sesión como administrador en vCenter Server.
   b. Desplácese hasta **Inicio > Administración > Inicio de sesión único > Configuración**.
   c. Haga clic en **Cambiar proveedor** y seleccione **Okta**.

      Se abrirá el asistente **Configurar proveedor de identidad principal**.
   d. En el panel **Requisitos previos**, revise los requisitos de Okta y de vCenter Server.
   e. Haga clic en **Ejecutar comprobaciones previas**.

      Si la comprobación previa encuentra errores, haga clic en **Ver detalles** y siga los pasos para resolver los errores como se indica.
   f. Cuando se apruebe la comprobación previa, haga clic en la casilla de confirmación y, a continuación, haga clic en **Siguiente**.

g En el panel **Información del directorio**, introduzca los siguientes datos.

- Nombre de directorio: nombre del directorio local que se va a crear en vCenter Server y que almacena los usuarios y los grupos insertados desde Okta. Por ejemplo, **`vcenter-okta-directory`**.
- Nombres de dominio: introduzca los nombres de dominio de Okta que contienen los usuarios y grupos de Okta que desea sincronizar con vCenter Server.

  Después de introducir el nombre de dominio de Okta, haga clic en el icono más (+) para agregarlo. Si introduce varios nombres de dominio, especifique el dominio predeterminado.

h Haga clic en **Siguiente**.

i En el panel **OpenID Connect**, introduzca la siguiente información.

- Interfaz de usuario de redireccionamiento: se rellena automáticamente. Proporcione la interfaz de usuario de redireccionamiento al administrador de Okta para usarla en la creación de la aplicación OpenID Connect.
- Nombre del proveedor de identidad: se rellena automáticamente como Okta.
- Identificador de cliente: se obtiene al crear la aplicación OpenID Connect en Okta en el paso 1. (Okta hace referencia al Identificador de cliente como ID de cliente).
- Secreto compartido: obtenido al crear la aplicación OpenID Connect en Okta en el paso 1. (Okta se refiere al secreto compartido como secreto de cliente).
- Dirección de OpenID: adopta el formato https://*Okta domain space*/oauth2/default/.well-known/openid-configuration.

  Por ejemplo, si su espacio de dominio Okta es example.okta.com, entonces la dirección de OpenID es: `https://example.okta.com/oauth2/default/.well-known/openid-configuration`

  Consulte https://developer.okta.com/docs/reference/api/oidc/#well-known-openid-configuration para obtener más información.

j Haga clic en **Siguiente**.

k Revise la información y haga clic en **Finalizar**.

vCenter Server crea el proveedor de identidad de Okta y muestra la información de configuración.

l Si es necesario, desplácese hacia abajo y haga clic en el icono **Copiar** del URI de redireccionamiento y guárdelo en un archivo.

El URI de redirección se utiliza en la aplicación Okta OpenID Connection.

m Haga clic en el icono **Copiar** de la URL del tenant y guárdela en un archivo.

Nota Si su red no es de acceso público; debe crear un túnel de red entre el sistema vCenter Server y el servidor Okta. Después de crear el túnel de red, utilice la URL de acceso público adecuada como URI base.

n En **Aprovisionamiento de usuarios**, haga clic en **Generar** para crear el token secreto, seleccione la duración del token en el menú desplegable y, a continuación, haga clic en **Copiar en el portapapeles**. Guarde el token en una ubicación segura.

Utilice la URL del tenant y el token en la aplicación SCIM 2.0 de Okta. La aplicación SCIM 2.0 de Okta utiliza el token para sincronizar los usuarios y grupos de Okta en VMware Identity Services. Esta información es necesaria para transferir usuarios y grupos de Okta a vCenter Server.

3 Vuelva al artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/90835 para actualizar el URI de redireccionamiento de Okta.

Siga los pasos de la sección titulada "Actualizar el URI de redireccionamiento de Okta".

4 Para crear la aplicación SCIM 2.0, continúe en el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/90835.

Siga los pasos de la sección titulada "Crear la aplicación SCIM 2.0 e insertar usuarios y grupos en vCenter Server".

Cuando termine de crear la aplicación SCIM 2.0 como se describe en el artículo de la base de conocimientos, continúe con el siguiente paso.

5 Configure vCenter Server para la autorización de Okta.

Puede asignar usuarios de Okta a un grupo de vCenter Server o asignar permisos globales y de nivel de inventario a los usuarios de Okta. El permiso mínimo necesario para iniciar sesión es de solo lectura.

Para asignar usuarios de Okta a un grupo, consulte Agregar miembros a un grupo de vCenter Single Sign-On. Para asignar permisos globales y de nivel de inventario a los usuarios de Okta, consulte el tema sobre la administración de permisos para los componentes de vCenter Server en la documentación de *Seguridad de vSphere*.

6 Confirme que se puede iniciar sesión en vCenter Server con un usuario de Okta.

Configurar la federación de proveedores de identidad de vCenter Server para Microsoft Entra ID

Después de instalar o actualizar a vSphere 8.0 Update 2 o versiones posteriores, puede configurar la federación de proveedores de identidad de vCenter Server para Microsoft Entra ID (anteriormente denominada Azure AD) como proveedor de identidad externo.

vCenter Server admite solo un proveedor de identidad externo configurado y el origen de identidad vsphere.local (fuente local). No se pueden utilizar varios proveedores de identidad externos. La federación de proveedores de identidad de vCenter Server usa OpenID Connect (OIDC) para los inicios de sesión del usuario en vCenter Server.

Puede configurar privilegios mediante usuarios y grupos de Microsoft Entra ID a través de permisos globales o de objetos en vCenter Server. Consulte la documentación de *Seguridad de vSphere* para obtener más información sobre cómo agregar permisos.

Para obtener una revisión del proceso de configuración, consulte el siguiente video:

Autenticación de vCenter: Integración de Azure AD/Entra ID | vSphere 8 Update 2

Requisitos previos

Requisitos de Microsoft Entra ID:

- Es cliente de Microsoft y tiene una cuenta de Microsoft Entra ID.

Requisitos de conectividad de Microsoft Entra ID:

- Creó una aplicación empresarial (no una galería) con OpenID Connect como un método de inicio de sesión.
- Agregue código de autorización, token de actualización y contraseña de propietario de recursos como tipos de concesión en la aplicación creada.
- Para la sincronización de usuarios y grupos, debe configurar el aprovisionamiento de la aplicación Galería de VMware Identity Services para SCIM 2.0 en Microsoft Entra ID con un token de portador de OAuth 2.0.

Requisitos de vCenter Server:

- vSphere 8.0 Update 2 o una versión posterior, con VMware Identity Services activado (se activan de forma predeterminada).
- En la instancia de vCenter Server donde desea crear el origen de identidad de Microsoft Entra ID, compruebe que VMware Identity Services esté activado.
- Los usuarios y los grupos del proveedor de identidad se aprovisionan en su instancia de vCenter Server.

Requisitos de privilegios de vSphere:

- Debe tener el privilegio **VcIdentityProviders.Manage** para crear, actualizar o eliminar un proveedor de identidad de vCenter Server que es necesario para la autenticación federada. Para limitar un usuario de forma que solamente pueda ver la información de configuración del proveedor de identidad, asigne el privilegio **VcIdentityProviders.Read**.

Requisitos de Enhanced Linked Mode:

- Puede configurar la federación de proveedores de identidad de vCenter Server para Microsoft Entra ID en una configuración de Enhanced Linked Mode. Cuando configure Microsoft Entra ID en Enhanced Link Mode, se configurará el proveedor de identidad de Microsoft Entra ID para que utilice VMware Identity Services en un único sistema vCenter Server. Por ejemplo, si la configuración de Enhanced Mode Link consta de dos sistemas vCenter Server, solo se utilizará una instancia de vCenter Server y su instancia de VMware Identity Services para comunicarse con el servidor de Microsoft Entra ID. Si este sistema de vCenter Server deja de estar disponible, puede configurar VMware Identity Services en otros sistemas de vCenter Server en la configuración de ELM para interactuar con el servidor de Microsoft Entra ID. Para obtener más información, consulte Proceso de activación para proveedores de identidad externos en configuraciones de Enhanced Linked Mode.
- Al configurar Microsoft Entra ID como proveedor de identidad externo, todos los sistemas de vCenter Server en una configuración de Enhanced Linked Mode deben ejecutar al menos vSphere 8.0 Update 2.

Requisitos de red:

- Si la red no es de acceso público, debe crear un túnel de red entre el sistema de vCenter Server y el servidor de Microsoft Entra ID y, a continuación, utilizar la URL de acceso público adecuada como URI base.

Procedimiento

1 Cree una aplicación de OpenID Connect en Microsoft Entra ID y asigne grupos y usuarios a la aplicación OpenID Connect.

   Para crear la aplicación OpenID Connect y asignar grupos y usuarios, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/94182. Siga los pasos de la sección titulada "Crear la aplicación OpenID Connect". Después de crear la aplicación OpenID Connect, copie la siguiente información de la aplicación OpenID Connect de Microsoft Entra ID en un archivo para usarlo al configurar el proveedor de identidad de vCenter Server en el siguiente paso.

   - Identificador de cliente
   - Secreto de cliente (que se muestra como secreto compartido en vSphere Client).
   - Información de dominio de Active Directory o información de dominio de Microsoft Entra ID si no está ejecutando Active Directory.

2 Para crear el proveedor de identidad en vCenter Server:

   a Utilice vSphere Client para iniciar sesión como administrador en vCenter Server.

   b Desplácese hasta **Inicio > Administración > Inicio de sesión único > Configuración**.

   c Haga clic en **Cambiar proveedor** y seleccione **Microsoft Entra ID**.

      Se abrirá el asistente **Configurar proveedor de identidad principal**.

d En el panel **Requisitos previos**, revise los requisitos de Microsoft Entra ID y de vCenter Server.

e Haga clic en **Ejecutar comprobaciones previas**.

Si la comprobación previa encuentra errores, haga clic en **Ver detalles** y siga los pasos para resolver los errores como se indica.

f Cuando se apruebe la comprobación previa, haga clic en la casilla de confirmación y, a continuación, haga clic en **Siguiente**.

g En el panel **Información del directorio**, introduzca los siguientes datos.

- Nombre de directorio: nombre del directorio local que se va a crear en vCenter Server y que almacena los usuarios y los grupos insertados desde Microsoft Entra ID. Por ejemplo, **`vcenter-entraid-directory`**.
- Nombres de dominio: introduzca los nombres de dominio de Microsoft Entra ID que contienen los usuarios y grupos de Microsoft Entra ID que desea sincronizar con vCenter Server.

  Después de introducir el nombre de dominio de Microsoft Entra ID, haga clic en el icono más (+) para agregarlo. Si introduce varios nombres de dominio, especifique el dominio predeterminado.

h Haga clic en **Siguiente**.

i En el panel **OpenID Connect**, introduzca la siguiente información.

- Interfaz de usuario de redireccionamiento: se rellena automáticamente. Proporcione la interfaz de usuario de redireccionamiento al administrador de Microsoft Entra ID para usarla en la creación de la aplicación OpenID Connect.
- Nombre del proveedor de identidad: se rellena automáticamente como Microsoft Entra ID.
- Identificador de cliente: se obtiene al crear la aplicación OpenID Connect en Microsoft Entra ID en el paso 1. (Microsoft Entra ID se refiere al identificador de cliente como ID de cliente).
- Secreto compartido: se obtiene al crear la aplicación OpenID Connect en Microsoft Entra ID en el paso 1. (Microsoft Entra ID se refiere al secreto compartido como secreto de cliente).
- Dirección de OpenID: adopta el formato https://*Microsoft Entra ID domain space*/oauth2/default/.well-known/openid-configuration.

  Por ejemplo, si su espacio de dominio de Microsoft Entra ID es example.EntraID.com, entonces la dirección de OpenID es: `https://example.EntraID.com/oauth2/default/.well-known/openid-configuration`

j Haga clic en **Siguiente**.

k Revise la información y haga clic en **Finalizar**.

vCenter Server crea el proveedor de identidad de Microsoft Entra ID y muestra la información de configuración.

l Si es necesario, desplácese hacia abajo y haga clic en el icono **Copiar** del URI de redireccionamiento y guárdelo en un archivo.

El URI de redirección se utiliza en la aplicación OpenID Connection de Microsoft Entra ID.

m Haga clic en el icono **Copiar** de la URL del tenant y guárdela en un archivo.

Nota Si su red no es de acceso público, debe crear un túnel de red entre el sistema de vCenter Server y el servidor de Microsoft Entra ID. Después de crear el túnel de red, utilice la URL de acceso público adecuada como URI base.

n En **Aprovisionamiento de usuarios**, haga clic en **Generar** para crear el token secreto, seleccione la duración del token en el menú desplegable y, a continuación, haga clic en **Copiar en el portapapeles**. Guarde el token en una ubicación segura.

Utilice la URL del tenant y el token en la aplicación SCIM 2.0 de Microsoft Entra ID. La aplicación SCIM 2.0 de Microsoft Entra ID utiliza el token para sincronizar los usuarios y grupos de Microsoft Entra ID en VMware Identity Services. Esta información es necesaria para transferir usuarios y grupos de Microsoft Entra ID a vCenter Server.

3 Vuelva al artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/94182 para actualizar el URI de redireccionamiento de Microsoft Entra ID.

Siga los pasos de la sección titulada "Actualizar el URI de redireccionamiento de Azure AD".

4 Para crear la aplicación SCIM 2.0, continúe en el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/94182.

Siga los pasos de la sección titulada "Crear la aplicación SCIM 2.0 e insertar usuarios y grupos en vCenter Server".

Cuando termine de crear la aplicación SCIM 2.0 como se describe en el artículo de la base de conocimientos, continúe con el siguiente paso.

5 Configure la pertenencia a grupos en vCenter Server para la autorización de Microsoft Entra ID.

Debe configurar la pertenencia a grupos para que los usuarios de Microsoft Entra ID puedan iniciar sesión en vCenter Server.

a En vSphere Client, cuando haya iniciado sesión como administrador local, vaya a **Administración > Inicio de sesión único > Usuarios y grupos**.

b Haga clic en la pestaña **Grupos**.

c Haga clic en el grupo **Administradores** y, a continuación, en **Agregar miembros**.

d Seleccione el nombre de dominio del grupo de Microsoft Entra ID que desea agregar en el menú desplegable.

e En el cuadro de texto que se encuentra debajo del menú desplegable, introduzca los primeros caracteres del grupo de Microsoft Entra ID que desea agregar y, a continuación, espere a que aparezca la selección desplegable.

f Seleccione el grupo de Microsoft Entra ID y agréguelo al grupo Administradores.

g Haga clic en **Guardar**.

6 Confirme que se puede iniciar sesión en vCenter Server con un usuario de Microsoft Entra ID.

7 Para asignar permisos globales y de nivel de inventario a los usuarios de Microsoft Entra ID, consulte el tema sobre la administración de permisos para los componentes de vCenter Server en la documentación de *Seguridad de vSphere*.

Configurar el proveedor de identidad de vCenter Server para PingFederate

Después de instalar o actualizar a vSphere 8.0 Update 3, puede configurar la federación de proveedores de identidad de vCenter Server para PingFederate como proveedor de identidad externo.

Pasos detallados de configuración del proveedor de identidad de vCenter Server para PingFederate

La configuración de vCenter Server para PingFederate implica los siguientes pasos detallados:

1 En PingFederate, cree la configuración específica de vCenter Server/VMware Identity Services, incluidos los ámbitos y la configuración común para los flujos de trabajo de PingFederate.

2 En PingFederate, cree elementos globales, como la configuración de flujo de concesión de contraseña y la configuración de flujo de código de autorización.

3 En PingFederate, instale el aprovisionador de SCIM.

4 En vCenter Server, cree el proveedor de identidad de PingFederate.

5 En PingFederate, cree la aplicación SCIM (conexión de SP).

6 En vCenter Server, autorice a los usuarios de PingFederate.

Nota Con las instrucciones de esta documentación, se crea una configuración típica para el servidor PingFederate. El entorno puede ser diferente y, por lo tanto, es posible que usted realice diferentes selecciones.

Requisitos previos para configurar el proveedor de identidad de vCenter Server para PingFederate

Requisitos de PingFederate:

- Instaló un servidor PingFederate local.

- Desde la instancia de vCenter Server donde configura el proveedor de identidad de PingFederate, debe obtener los certificados raíz de confianza e importarlos al servidor PingFederate.
- De forma opcional, es posible que deba importar el certificado SSL de PingFederate, o cadena de certificados, a vCenter Server, si ese certificado está autofirmado (es decir, no emitido por una entidad de certificación pública conocida). Si el certificado SSL de PingFederate o uno de los certificados de la cadena fue emitido por una entidad de certificación conocida, vCenter Server automáticamente confía en ese certificado y no es necesario importarlo. Si utiliza una o varias entidades de firma intermedias para el certificado SSL del servidor PingFederate, incluya la cadena completa de certificados.

  Para exportar el certificado SSL de PingFederate, en la consola administrativa de PingFederate, vaya a **Seguridad > Certificados de servidor de SSL**, seleccione el certificado predeterminado y elija **Exportar** en el menú desplegable **Seleccionar acción**.

  El certificado SSL de PingFederate se importa mediante vSphere Client en el panel **OpenID Connect** como parte del flujo de trabajo de configuración del proveedor de identidad.
- Para realizar inicios de sesión en OIDC y administrar permisos de usuario y grupo, debe crear las siguientes aplicaciones de PingFederate.
  - Una aplicación nativa de PingFederate con OpenID Connect como método de inicio de sesión. La aplicación nativa debe incluir los tipos de concesión de código de autorización, token de actualización y contraseña del propietario del recurso.
  - Una aplicación de Sistema para la administración de identidades entre dominios (SCIM) (en PingFederate, se denomina Conexión de SP) 2.0 con un token de portador OAuth 2.0 para realizar la sincronización de usuarios y grupos entre el servidor de PingFederate y vCenter Server.
- Identificó los usuarios y grupos de PingFederate que desea compartir con vCenter Server. Este uso compartido es una operación SCIM (no una operación OIDC).

Requisitos de conectividad de PingFederate:

- vCenter Server debe poder conectarse al endpoint de detección de PingFederate y a los endpoints de autorización, token, JWKS y de cualquier otra índole que estén anunciado en los metadatos de endpoint de detección.
- PingFederate debe poder conectarse con vCenter Server para enviar datos de usuarios y grupos para el aprovisionamiento de SCIM.

Requisitos de vCenter Server:

- vSphere 8.0 Update 3

- En la instancia de vCenter Server donde desea crear el origen de identidad de PingFederate, compruebe que VMware Identity Services esté activado.

  Nota Al instalar o actualizar a vSphere 8.0 Update 1 o una versión posterior, los servidores de identidad de VMware se activan de forma predeterminada. Puede utilizar la interfaz de administración de vCenter Server para confirmar el estado de VMware Identity Services. Consulte Detener e iniciar VMware Identity Services.

Requisitos de privilegios de vSphere:

- Debe tener el privilegio **VcIdentityProviders.Administrar** para crear, actualizar o eliminar un proveedor de identidad de vCenter Server que es necesario para la autenticación federada. Para limitar un usuario de forma que solamente pueda ver la información de configuración del proveedor de identidad, asigne el privilegio **VcIdentityProviders.Leer**.

Requisitos de Enhanced Linked Mode:

- Puede configurar la federación de proveedores de identidad de vCenter Server para PingFederate en una configuración de Enhanced Linked Mode. Cuando configure PingFederate en Enhanced Link Mode, se configurará el proveedor de identidad de PingFederate de modo que utilice VMware Identity Services en un único sistema de vCenter Server. Por ejemplo, si la configuración de Enhanced Mode Link consta de dos sistemas de vCenter Server, solo se utilizará una instancia de vCenter Server y su instancia de VMware Identity Services para comunicarse con el servidor PingFederate. Si este sistema de vCenter Server deja de estar disponible, puede configurar VMware Identity Services en otra instancia de vCenter Server de la configuración de ELM para interactuar con el servidor de PingFederate. Para obtener más información, consulte Proceso de activación para proveedores de identidad externos en configuraciones de Enhanced Linked Mode.
- Al configurar PingFederate como proveedor de identidad externo, todos los sistemas de vCenter Server en una configuración de Enhanced Linked Mode deben ejecutar al menos vSphere 8.0 Update 3.

Qué leer a continuación

Procedimiento

1 Crear los ámbitos

  PingFederate admite el uso de ámbitos para restringir y definir los privilegios de acceso.

2 Crear una configuración común para flujos de trabajo de PingFederate

  La creación de la configuración común para PingFederate incluye la creación del administrador de tokens de acceso, el atributo objectID, la directiva de OpenID Connect y la aplicación cliente de OAuth.

3 Crear la configuración de flujo de concesión de contraseña

  Para que PingFederate se autentique con vCenter Server, configure el flujo de concesión de contraseña.

4 Crear la configuración del flujo de código de autorización

La creación del flujo de código de autorización en PingFederate implica crear y configurar un adaptador de IdP.

5 Instalar el aprovisionador de SCIM

Debe crear un sistema para la aplicación del Sistema para la administración de identidades entre dominios (SCIM) que utilice un token a fin de sincronizar los grupos y usuarios de PingFederate en VMware Identity Services.

6 Configurar la federación de proveedores de identidad de vCenter Server para PingFederate

Después de instalar o actualizar a vSphere 8.0 Update 3, puede configurar la federación de proveedores de identidad de vCenter Server para PingFederate como proveedor de identidad externo.

7 Crear la aplicación de SCIM (conexión de SP)

Es necesario crear un sistema para la aplicación de administración de identidades entre dominios (SCIM) 2.0, de modo que pueda especificar qué usuarios y grupos de PingFederate desea insertar en vCenter Server.

8 Configurar vCenter Server para la autorización de PingFederate

Puede asignar usuarios de PingFederate a un grupo de vCenter Server o asignar permisos globales y de nivel de inventario a los usuarios de PingFederate.

Crear los ámbitos

PingFederate admite el uso de ámbitos para restringir y definir los privilegios de acceso.

Requisitos previos

Consulte Requisitos previos para configurar el proveedor de identidad de vCenter Server para PingFederate.

Inicie sesión en la consola de administrador de PingFederate con una cuenta de administrador.

Procedimiento

1 Vaya a **Sistema > Configuración de OAuth > Administración de ámbitos**.

2 En la pestaña **Ámbitos comunes**, agregue los siguientes **valores de ámbito** junto con una descripción. Haga clic en **Agregar** después de introducir cada valor y descripción.

   - **openid**
   - **perfil**
   - **email**

3 Omita la pestaña **Ámbitos exclusivos**.

4 En la pestaña **Ámbito predeterminado**, introduzca una descripción para **Ámbito predeterminado**.

Se requiere una descripción. Si **Descripción del ámbito predeterminado** está vacío, PingFederate registra el siguiente error:

El ámbito solicitado no es válido, es desconocido, tiene un formato incorrecto o supera el que el cliente puede solicitar.

5 Haga clic en **Guardar**.

Pasos siguientes

Continúe con Crear una configuración común para flujos de trabajo de PingFederate.

Crear una configuración común para flujos de trabajo de PingFederate

La creación de la configuración común para PingFederate incluye la creación del administrador de tokens de acceso, el atributo objectID, la directiva de OpenID Connect y la aplicación cliente de OAuth.

Requisitos previos

Realice la siguiente tarea:

- Crear los ámbitos

Inicie sesión en la consola de administrador de PingFederate con una cuenta de administrador.

Procedimiento

1 Cree el administrador de tokens de acceso.

   a Vaya a **Aplicaciones > Oauth > Administración de token de acceso**.

   b Haga clic en **Crear nuevas licencias**.

   c En la pestaña **Tipo**:

      - **Nombre de instancia**, introduzca un nombre de instancia. Por ejemplo, vIDB Access Token Manager.
      - **Id. de instancia**: introduzca el identificador de instancia. Por ejemplo, vIDB.
      - **Tipo**: seleccione **JSON Web Tokens**.
      - **Instancia principal**: deje el valor predeterminado, **Ninguna**.

d En la pestaña **Configuración de instancia**:

- **Usar clave de firma centralizada**, seleccione la casilla de verificación.

  Si se deja esta casilla de verificación sin seleccionar, PingFederate esperará que se configure "Identificador de clave de certificado de firma activa".

- **Algoritmo de JWS**: seleccione un algoritmo. Por ejemplo, **RSA con SHA-256**.
- En la parte inferior de la pantalla, haga clic en **Mostrar campos avanzados**.
  - **Longitud de notificación de identificador de JWT**: agregue un número mayor que cero (0). Por ejemplo, 24. Si no introduce un valor, la notificación JTI se omite en el token de acceso.

e Haga clic en **Siguiente**.

f En la pestaña **Contrato de atributo de token de acceso**:

- En el cuadro de texto **Ampliar el contrato**, agregue las siguientes notificaciones que se generarán en el token de acceso de ping. Haga clic en **Agregar** después de introducir cada notificación.
  - **aud**
  - **iss**
  - **exp**
  - **iat**
  - **userName**
- **Nombre de atributo del sujeto**: seleccione una notificación que se utilizará para fines de auditoría. Por ejemplo, **iss**.

g Haga clic en **Siguiente** dos veces para omitir las pestañas **URI de recurso** y **Control de acceso**.

h Haga clic en **Guardar**.

2 Agregue el atributo objectGUID.

a Vaya a **Sistema > Almacenes de datos >** *Su almacén de datos* **> Configuración de LDAP**.

b En la pestaña **Configuración de LDAP**, haga clic en **Avanzada** en la parte inferior.

c En la pestaña **Atributos binarios de LDAP**, en el campo de nombre **Atributo binario**, utilice **objectGUID** y haga clic en **Agregar**.

d Haga clic en **Guardar**.

3 Cree la directiva de OpenID Connect.

a Vaya a **Aplicaciones > Oauth > Administración de políticas de OpenID Connect**.

b Haga clic en **Agregar directiva**.

c En la pestaña **Gestionar directiva**:

- **Id. de directiva**: introduzca un identificador de directiva. Por ejemplo, OIDC.
- **Nombre**: introduzca un nombre de directiva. Por ejemplo, Directiva de OIDC.
- **Administrador de tokens de acceso**: seleccione el administrador de tokens de acceso que creó anteriormente. Por ejemplo, vIDB Access Token Manager.

d Haga clic en **Siguiente**.

e En la pestaña **Contrato de atributo**:

- Haga clic en **Eliminar** para eliminar todos los atributos, excepto **sub**. De lo contrario, debe asignar los atributos a un valor en la pestaña **Cumplimiento de contrato** más adelante.

f Haga clic en **Siguiente** y, a continuación, haga clic de nuevo en **Siguiente** para omitir la pestaña **Ámbito de atributos**.

g En la pestaña **Orígenes de atributos y búsqueda de usuarios**, haga clic en **Agregar origen de atributo**.

Después de introducir la información en cada pestaña que aparece a continuación, haga clic en **Siguiente** para avanzar.

- **Almacén de datos**:
  - **Id. de origen de atributo**: introduzca un identificador de origen de atributo. Por ejemplo, vIDBLDAP.
  - **Descripción del origen del atributo**: introduzca una descripción. Por ejemplo: vIDBLDAP.
  - **Almacén de datos activo**: seleccione Active Directory o el nombre de dominio de OpenLDAP en el menú desplegable.
- **Búsqueda del directorio LDAP**:
  - **DN base**: introduzca el DN base para buscar usuarios y grupos.
  - **Ámbito de búsqueda**: deje el valor predeterminado, **Subtree**.
  - **Atributos para devolver desde la búsqueda**: seleccione **<Mostrar todos los atributos>** y seleccione **objectGUID**.

    Haga clic en **Agregar atributo**.
- **Tipos de codificación de atributos binarios de LDAP**:
  - **ObjectGUID**: seleccione **Hex** para el **Tipo de codificación de atributo**.
- **Filtro LDAP**:
  - **Filtro**: introduzca un filtro. Por ejemplo, `userPrincipalName=${userName}`.

h En la página **Resumen**, haga clic en **Listo**.

i Haga clic en **Siguiente** para avanzar y, en la pestaña **Cumplimiento de contrato**, asigne el **Contrato de atributos** para el token de identificador:

Contrato de atributo	Origen	Valor
sub	Seleccione el identificador de origen del atributo creado anteriormente. En esta documentación, el ejemplo utilizado es vIDBLDAP.	**objectGUID**

j Haga clic en **Siguiente** y, a continuación, haga clic en **Siguiente** de nuevo para omitir la pestaña **Criterios de seguro**.

k Haga clic en **Guardar**.

4 Cree la aplicación cliente de OAuth.

a Vaya a **Aplicaciones > Oauth > Clientes**.

b Haga clic en **Agregar cliente**.

c En la página **Clientes | Cliente**:

- **ID de cliente**: introduzca el identificador de cliente. Por ejemplo, vIDB.

  Nota Copie y guarde el ID de cliente si desea usarlo más adelante al crear el proveedor de identidad de vCenter Server para PingFederate.

- **Nombre**: introduzca un nombre. Por ejemplo, vIDB.
- **Autenticación de cliente**: seleccione **Secreto de cliente**.
  - **Secreto de cliente**: puede introducir su propio secreto de cliente o generar un secreto. Una vez que abandone esta página, no podrá ver el secreto generado. Solo tiene la opción de cambiar el secreto.

    Nota Copie y guarde el secreto para usarlo más adelante al crear el proveedor de identidad de vCenter Server.

- **URI de redireccionamiento**: introduzca los URI de redireccionamiento con el formato **`https://`*`vCenter_Server_FQDN`*`:port/federation/t/CUSTOMER/auth/response/oauth2`**.
  - Haga clic en **Agregar**.
- **Tipos de concesión permitidos**: compruebe el **Código de autenticación**, **Token de actualización**, **Credenciales de cliente** y **Credenciales de contraseña de propietario del origen**.
- **Administrador de tokens de acceso predeterminado**: seleccione el administrador de tokens de acceso que creó anteriormente. Por ejemplo, el que se utiliza en esta documentación es vIDB Access Token Manager.
- **OpenID Connect**: para **Directiva**, seleccione la que creó anteriormente. Por ejemplo, la que se utiliza en esta documentación es OIDC.

d Haga clic en **Guardar**.

Pasos siguientes

Continúe con Crear la configuración de flujo de concesión de contraseña.

Crear la configuración de flujo de concesión de contraseña

Para que PingFederate se autentique con vCenter Server, configure el flujo de concesión de contraseña.

Requisitos previos

Realice las siguientes tareas:

- Crear los ámbitos
- Crear una configuración común para flujos de trabajo de PingFederate

Inicie sesión en la consola de administrador de PingFederate con una cuenta de administrador.

Procedimiento

1 Cree el validador de credenciales de contraseña.

   a Vaya a **Sistema > Almacenamiento de datos y credenciales > Validadores de credenciales de contraseña**.

   b Haga clic en **Crear nuevas licencias**.

   c En la página **Validadores de credenciales de contraseña | Crear nueva instancia**, introduzca la información de la siguiente manera para cada pestaña y, a continuación, haga clic en **Siguiente** para avanzar.

      - En la pestaña **Tipo**:
         - **Nombre de instancia**: introduzca el nombre de la instancia. Por ejemplo, Validador vIDB.
         - **Id. de instancia**: introduzca el identificador de instancia. Por ejemplo, vIDB.
         - **Tipo**: seleccione Validador de credenciales de contraseña de nombre de usuario de LDAP.
      - En la pestaña **Configuración de instancia**:
         - **Almacén de datos de LDAP**: seleccione el almacén de datos que está utilizando.
         - **Buscar base**: introduzca el DN base para buscar usuarios y grupos.
         - **Filtro de búsqueda**: introduzca un filtro. Por ejemplo, `userPrincipalName=${username}`.
         - **Ámbito de búsqueda**: seleccione **subárbol**.
      - En la pestaña **Contrato ampliado**:
         - De forma predeterminada, se agrega lo siguiente:
            - **DN**
            - **email**
            - **givenName**
            - **username**

   d Haga clic en **Siguiente**, y, a continuación, haga clic en **Guardar**.

2 Asigne el validador en la configuración del servidor de autorización.

   a Vaya a **Sistema > Ajustes de Oauth > Ajustes del servidor de autorización**.

   b En **Validador de credenciales de contraseña**, seleccione el que creó anteriormente. Por ejemplo, en esta documentación se utiliza el validador vIDB.

   c Haga clic en **Guardar**.

3 Cree la asignación de concesión de credenciales del propietario del recurso.

a Vaya a **Autenticación > Oauth > Asignación de credenciales del propietario del recurso**.

b En la ventana **Asignación de credenciales del propietario del recurso**:

- **Instancia del validador de contraseña de origen**: seleccione la que creó anteriormente y haga clic en **Agregar asignación**.

c En la página **Asignación de concesión de credenciales del propietario del recurso | Asignación de credenciales del propietario del recurso**, haga clic en **Siguiente** para omitir la pestaña **Orígenes de atributos y búsqueda de usuarios**.

d En la pestaña **Cumplimiento del contrato**:

- En **USER_KEY**, seleccione Validador de credenciales de contraseña y en **Valor**, seleccione **username**.

e Haga clic en **Siguiente** para omitir la pestaña **Criterios de seguro** y, a continuación, haga clic en **Guardar**.

4 Crear la asignación de token de acceso: asigne el validador de credenciales de contraseña al administrador de tokens de acceso.

Esta asignación es necesaria para el flujo de trabajo de la concesión de contraseña. Si la asignación no existe, PingFederate registra el siguiente error:

No hay administradores de token de acceso disponibles para el cliente y el contexto de autenticación seleccionados.

a Vaya a **Aplicaciones > Asignación de token de acceso**.

- **Contexto**: seleccione el que creó anteriormente. Por ejemplo, en esta documentación se utiliza el validador vIDB.
- **Administrador de tokens de acceso**: seleccione el que creó anteriormente. Por ejemplo, en esta documentación se utiliza el administrador de tokens de acceso vIDB.

b Haga clic en **Agregar asignación**.

c Haga clic en **Siguiente** para omitir la pestaña **Orígenes de atributos y búsqueda de usuarios**.

d En la pestaña **Cumplimiento del contrato**, utilice la siguiente tabla.

Contrato	Origen	Valor
aud	**Contexto**	El identificador de cliente creado previamente. Por ejemplo, el identificador utilizado en esta documentación es vIDB.
exp	**Sin asignación**	-
iat	**Expresión**	Introduzca lo siguiente: `@org.jose4j.jwt.NumericDate@now().getValue()`
iss	**Expresión** (Si no está visible, consulte la documentación de PingFederate en https://docs.pingidentity.com/r/en-us/pingfederate-120/pf_enable_disable_express).	Introduzca lo siguiente: `#tmp=#this.get("context.HttpRequest").getObjectValue().getRequestURL().toString(), #url=new java.net.URL(#tmp), #protocol=#url.getProtocol(), #host=#url.getHost(),#port=#url.getPort(), #result=(#port != -1) ? @java.lang.String@format("%s://%s:%d", #protocol, #host, #port) : @java.lang.String@format("%s://%s", #protocol, #host, #port)`
userName	**Sin asignación**	- Este contrato se utiliza más adelante en el filtro de LDAP para el flujo de trabajo de la directiva de OIDC para el código de autorización. En el caso del flujo de trabajo de PingFederate, no es necesario.

e Haga clic en **Siguiente** para omitir la pestaña **Criterios de seguro** y, a continuación, haga clic en **Guardar**.

Pasos siguientes

Continúe con Crear la configuración del flujo de código de autorización.

Crear la configuración del flujo de código de autorización

La creación del flujo de código de autorización en PingFederate implica crear y configurar un adaptador de IdP.

Requisitos previos

Realice las siguientes tareas:

- Crear los ámbitos
- Crear una configuración común para flujos de trabajo de PingFederate
- Crear la configuración de flujo de concesión de contraseña

Inicie sesión en la consola de administrador de PingFederate con una cuenta de administrador.

Procedimiento

1 Cree el adaptador de IdP.

   a Vaya a **Autenticación > Integración > Adaptadores de IdP**.

   b Haga clic en **Crear nueva instancia**.

   c En la pestaña **Tipo**:

   - **Nombre de instancia**: introduzca un nombre, por ejemplo, Adaptador de autenticación de formularios HTML.
   - **Identificador de instancia**: introduzca un identificador, por ejemplo, HTMLFormAuthAdapter.
   - **Tipo**: seleccione Adaptador de IdP de formulario HTML.
   - **Instancia principal**: seleccione **Ninguna**.

   d Haga clic en **Siguiente**.

   e En la pestaña **Adaptador de IdP**:

   En **Instancia del validador de credenciales de contraseña**, haga clic en **Agregar una nueva fila a "Validadores de credenciales".** A continuación, seleccione un validador (en esta documentación, se utiliza vIDB) y haga clic en **Actualizar**.

   f En la pestaña **Adaptador de IdP**:

   - **Dominio**: seleccione **USER_KEY**.

   g Haga clic en **Siguiente**.

   h Haga clic en **Siguiente** para omitir la pestaña **Contrato ampliado**.

   i En la pestaña **Atributos de adaptador**:

   - **Atributo de clave de usuario único**: seleccione **Nombre de usuario** y marque **Seudónimo**.

   j Haga clic en **Siguiente** para omitir la pestaña **Asignación de contrato de adaptador** y, a continuación, haga clic en **Guardar**.

2 Cree una asignación de concesión de adaptadores de IdP.

a Vaya a **Autenticación > Oauth > Asignación de concesión de adaptadores de IdP**.

b **Instancia de adaptador de origen**: seleccione la instancia de adaptador que acaba de crear y haga clic en **Agregar asignación**.

c En la página **Orígenes de atributos y búsqueda de usuarios**, haga clic en **Agregar origen de atributo**.

d Introduzca la siguiente información para cada pestaña y, a continuación, haga clic en **Siguiente** para avanzar.

- En la pestaña **Almacén de datos**:
  - **Identificador de origen de atributo**: introduzca un identificador con valores alfanuméricos.
  - **Descripción del origen del atributo**. Introduzca una descripción.
  - **Almacén de datos activo**: seleccione el directorio activo en uso.
- En la pestaña **Búsqueda del directorio LDAP**:
  - **DN base**: introduzca el DN base para buscar usuarios y grupos.
  - **Ámbito de búsqueda**: utilice el valor predeterminado, **Subtree**.
  - **Atributos para devolver desde la búsqueda**: seleccione **<Mostrar todos los atributos>** y, una vez cargados, en la lista de atributos, seleccione **userPrincipalName**.

e Haga clic en **Agregar atributo** y en **Siguiente**.

f En la pestaña **Filtro LDAP**:

- **Filtro**: introduzca el filtro. Por ejemplo, `userPrincipalName=${username}`.

g Haga clic en **Siguiente**, y, a continuación, haga clic en **Guardar**.

h En la página **Asignación de concesión de adaptadores de IdP | Asignación de adaptadores de IdP**, termine de crear la asignación de concesión de IdP.

En la pestaña **Búsqueda de cumplimiento de contratos**, utilice la siguiente tabla.

Contrato	Origen	Valor
USER_KEY	Seleccione el origen creado anteriormente.	DN de asunto
USER_NAME	Seleccione el origen creado anteriormente.	userPrincipalName

i Haga clic en **Siguiente**, y, a continuación, haga clic en **Guardar**.

La asignación de concesión de adaptadores de IdP creada se muestra como **'*Adapter Name*' en el Contrato de concesión persistente**.

3 Asigne el adaptador de IdP a Access Token Manager.

a Vaya a **Aplicaciones > Oauth > Asignaciones de token de acceso**.

- **Contexto**: seleccione **Adaptador de IdP:***Nombre de adaptador*.
- **Access Token Manager**: seleccione la instancia del administrador de tokens de acceso creada anteriormente. Por ejemplo, en esta documentación, es vIDB Access Token Manager.

b Haga clic en **Agregar asignación**.

Si no realiza esta asignación, PingFederate genera el siguiente mensaje de archivo de registro:

No hay fuentes de autenticación asignadas entre las que elegir. Asigne primero un adaptador de IdP o una conexión de IdP.

c Omita la pestaña **Orígenes de atributos y búsqueda de usuarios** y, en la pestaña **Cumplimiento de contrato**, utilice la siguiente tabla.

Contrato	Origen	Valor
aud	Sin asignación	-
exp	Sin asignación	-
iat	Sin asignación	-
iss	Sin asignación	-
userName	Adaptador	username

d Haga clic en **Siguiente** para omitir la pestaña **Criterios de seguro** y, a continuación, haga clic en **Guardar**.

Pasos siguientes

Continúe con Instalar el aprovisionador de SCIM.

Instalar el aprovisionador de SCIM

Debe crear un sistema para la aplicación del Sistema para la administración de identidades entre dominios (SCIM) que utilice un token a fin de sincronizar los grupos y usuarios de PingFederate en VMware Identity Services.

En el servidor de PingFederate, debe instalar el aprovisionador de SCIM para habilitar el aprovisionamiento de usuarios y grupos mediante SCIM.

Nota Si utiliza un entorno de PingFederate existente, es posible que ya tenga instalado el aprovisionador de SCIM.

Requisitos previos

Realice las siguientes tareas:

- Crear los ámbitos

- Crear una configuración común para flujos de trabajo de PingFederate
- Crear la configuración de flujo de concesión de contraseña
- Crear la configuración del flujo de código de autorización

Procedimiento

1 Descargue el aprovisionador de SCIM desde https://support.pingidentity.com/s/marketplace-integration/a7i1W0000004IDNQA2/scim-provisioner.

   Debe iniciar sesión en el portal de PingIdentity.

2 Copie el archivo `pf-scim-quickconnection-1.4.jar` en la carpeta que se encuentra montada en la carpeta `/opt/out` del servidor de PingFederate.

   Por ejemplo, coloque el archivo en la carpeta `/opt/out/instance/server/default/deploy`.

3 Consulte el archivo `/opt/out/instance/bin/run.properties` y asegúrese de que esta opción de configuración esté presente: `pf.provisioner.mode=STANDALONE`

   Según la documentación de PingFederate:

   INDEPENDIENTE: este servidor es una instancia independiente que ejecuta la consola de interfaz de usuario y el motor de protocolo (predeterminado).

4 Si la instancia del servidor de PingFederate se está ejecutando como una imagen de contenedor y actualizó el archivo `run.properties`, es posible que deba reiniciar el servidor. Por ejemplo:

   a Conéctese al servidor de PingFederate mediante SSH.

   b Cambie al directorio `/root/ping`.

   c Ejecute los siguientes comandos:

   ```
   docker-compose down
   docker-compose up
   ```

Resultados

El conector de SCIM se muestra como una opción al configurar el aprovisionamiento de usuarios en Crear la aplicación de SCIM (conexión de SP).

Pasos siguientes

Continúe con Configurar la federación de proveedores de identidad de vCenter Server para PingFederate.

Configurar la federación de proveedores de identidad de vCenter Server para PingFederate

Después de instalar o actualizar a vSphere 8.0 Update 3, puede configurar la federación de proveedores de identidad de vCenter Server para PingFederate como proveedor de identidad externo.

vCenter Server admite solo un proveedor de identidad externo configurado y el origen de identidad vsphere.local (fuente local). No se pueden utilizar varios proveedores de identidad externos. La federación de proveedores de identidad de vCenter Server usa OpenID Connect (OIDC) para los inicios de sesión del usuario en vCenter Server.

Puede configurar privilegios mediante usuarios y grupos de PingFederate a través de permisos globales o de objetos en vCenter Server. Consulte la documentación de *Seguridad de vSphere* para obtener más información sobre cómo agregar permisos.

Requisitos previos

Realice las siguientes tareas:

- Crear los ámbitos
- Crear una configuración común para flujos de trabajo de PingFederate
- Crear la configuración de flujo de concesión de contraseña
- Crear la configuración del flujo de código de autorización
- Instalar el aprovisionador de SCIM

Asegúrese de tener la siguiente información de la aplicación PingFederate OpenID Connect:

- Identificador de cliente
- Secreto de cliente (que se muestra como secreto compartido en vSphere Client)
- Información de dominio de Active Directory o información de dominio de PingFederate si no está ejecutando Active Directory

Procedimiento

1. Para crear el proveedor de identidad en vCenter Server:
   a. Utilice vSphere Client para iniciar sesión como administrador en vCenter Server.
   b. Vaya a **Inicio > Administración > Inicio de sesión único > Configuración**.
   c. Haga clic en **Cambiar proveedor** y seleccione **PingFederate**.

      Se abrirá el asistente **Configurar proveedor de identidad principal**.
   d. En el panel **Requisitos previos**, revise los requisitos de PingFederate y de vCenter Server, entre otros.

e Haga clic en **Ejecutar comprobaciones previas**.

Si la comprobación previa encuentra errores, haga clic en **Ver detalles** y siga los pasos para resolver los errores como se indica.

f Cuando se apruebe la comprobación previa, haga clic en la casilla de confirmación y, a continuación, haga clic en **Siguiente**.

g En el panel **Información del directorio**, introduzca los siguientes datos.

- Nombre de directorio: nombre del directorio local que se va a crear en vCenter Server y que almacena los usuarios y los grupos insertados desde PingFederate. Por ejemplo, **`vcenter-PingFederate-directory`**.
- Nombres de dominio: introduzca los nombres de dominio de PingFederate que contienen los usuarios y grupos de PingFederate que desea sincronizar con vCenter Server.

  Después de introducir el nombre de dominio de PingFederate, haga clic en el icono más (+) para agregarlo. Si introduce varios nombres de dominio, especifique el dominio predeterminado.

h Haga clic en **Siguiente**.

i En el panel **OpenID Connect**, introduzca la siguiente información.

- Interfaz de usuario de redireccionamiento: se rellena automáticamente. Esta interfaz de usuario de redireccionamiento debe coincidir con lo que se utiliza al crear la aplicación OpenID Connect en PingFederate.
- Nombre del proveedor de identidad: se rellena automáticamente como PingFederate.
- Identificador de cliente: se obtiene al crear la aplicación OpenID Connect. (PingFederate se refiere al identificador de cliente como ID de cliente).
- Secreto compartido: se obtiene al crear la aplicación OpenID Connect en PingFederate. (PingFederate se refiere al secreto compartido como secreto de cliente).
- Dirección de OpenID: tiene el formato https://*PingFederate_domain_space*/idp/.well-known/openid-configuration.

  Por ejemplo, si su espacio de dominio de PingFederate es example.PingFederate.com, entonces la dirección de OpenID es: `https://example.PingFederate.com/idp/.well-known/openid-config`
- Certificado SSL: como opción, si este certificado no ha sido emitido por una entidad de certificación pública y conocida, busque el certificado SSL de PingFederate o la cadena de certificados para cargarlo en vCenter Server. Para exportar el certificado SSL de PingFederate, en la consola de administración, vaya a **Seguridad > Certificados de servidor SSL**, seleccione el certificado predeterminado y elija **Exportar** en el menú desplegable **Seleccionar acción**. Para obtener más información, consulte el artículo Exportar un certificado, en https://docs.pingidentity.com/r/en-us/pingfederate-111/nfv1585678806463. Puede exportar el certificado SSL de PingFederate sin la clave privada, ya que no es necesario para la configuración de vCenter Server.

j Haga clic en **Siguiente**.

k Revise la información y haga clic en **Finalizar**.

vCenter Server crea el proveedor de identidad de PingFederate y muestra la información de configuración.

2 En **Aprovisionamiento de usuarios**, haga clic en **Generar** para crear el token secreto, seleccione la duración del token en el menú desplegable y, a continuación, haga clic en **Copiar en el portapapeles**. Guarde el token en una ubicación segura.

Al crear la conexión de procesador de almacenamiento (SP) de PingFederate (aplicación SCIM), se utiliza el token para sincronizar los usuarios y grupos de PingFederate en VMware Identity Services.

Pasos siguientes

Continúe con Crear la aplicación de SCIM (conexión de SP).

Crear la aplicación de SCIM (conexión de SP)

Es necesario crear un sistema para la aplicación de administración de identidades entre dominios (SCIM) 2.0, de modo que pueda especificar qué usuarios y grupos de PingFederate desea insertar en vCenter Server.

Requisitos previos

Realice las siguientes tareas:

- Crear los ámbitos
- Crear una configuración común para flujos de trabajo de PingFederate
- Crear la configuración de flujo de concesión de contraseña
- Crear la configuración del flujo de código de autorización
- Instalar el aprovisionador de SCIM
- Configurar la federación de proveedores de identidad de vCenter Server para PingFederate

Procedimiento

1 Agregue el certificado raíz de confianza de vCenter Server al servidor PingFederate.

   Antes de comenzar, exporte los certificados raíz de confianza desde vCenter Server. Puede obtener el certificado del sistema de archivos de vCenter Server en `/var/lib/vmware/vmca/root.cer`. O bien, consulte el artículo de la base de conocimientos en https://kb.vmware.com/s/article/2108294.

   a Inicie sesión en la consola de administrador de PingFederate con una cuenta de administrador.

   b Vaya a **Seguridad > Administración de certificados y claves**.

   c Seleccione **CA de confianza** y, a continuación, haga clic en **Importar** para agregar el certificado SSL de vCenter Server.

   d Si la instancia del servidor de PingFederate se está ejecutando como una imagen de contenedor, es posible que deba reiniciar el servidor para agregar el certificado al almacén de confianza. Por ejemplo:

      1 Conéctese al servidor de PingFederate mediante SSH.

      2 Cambie al directorio `/root/ping`.

      3 Ejecute los siguientes comandos:

      ```
      docker-compose down
      docker-compose up
      ```

2 Cree la conexión de SP.

a Inicie sesión en la consola de administrador de PingFederate con una cuenta de administrador.

b Vaya a **Aplicaciones > Integración > Conexiones de SP**.

c Haga clic en **Crear conexión**.

d Seleccione **Usar una plantilla para esta conexión** y, a continuación, seleccione **Conector de SCIM** en el menú desplegable.

Si la opción Conector de SCIM no aparece en el menú desplegable, compruebe que colocó el archivo `.jar` del conector de SCIM en la carpeta correcta (la carpeta `/opt/out` del servidor PingFederate).

e Haga clic en **Siguiente**.

f Seleccione solo **Aprovisionamiento saliente** y, luego, haga clic en **Siguiente**.

g En la pestaña **Información general**:

- **Id. de entidad del socio (identificador de conexión)**: actualice **Conector de SCIM** a un nombre de su elección.
- **Nombre de la conexión**: introduzca un nombre.
- **URL base**: introduzca la dirección HTTPS de vCenter Server en la que va a configurar el proveedor de identidad externo de PingFederate, por ejemplo: **`https://vcenter1.example.com`**.

h Haga clic en **Siguiente**.

i Haga clic en **Configurar aprovisionamiento**.

En la pestaña **Destino**:

- **URL de SCIM**: introduzca el endpoint del grupo de usuarios.

  Esta es la URL de tenant que se obtiene en **Aprovisionamiento del usuario** en la página **Configuración** de vCenter Server. Por ejemplo: **`https://vcenter1.example.com/usergroup/t/CUSTOMER/scim/v2`**
- **Método de autenticación**: seleccione **el token de portador de OAuth 2** en el menú desplegable.
- **Token de acceso**: pegue el token secreto que se generó desde vCenter Server y que debería haber guardado previamente. Consulte el paso 2 de Configurar la federación de proveedores de identidad de vCenter Server para PingFederate.
- **Identificador de usuario único**: seleccione **userName** en el menú desplegable.
- **Expresión de filtro**: copie la siguiente expresión en el cuadro de texto: **`externalId eq "%s"`**.

j Acepte el resto de los valores de configuración predeterminados y haga clic en **Siguiente**.

- **Opciones de aprovisionamiento**: **Creación de usuario**, **Actualización de usuario** y **Deshabilitación/Eliminación de usuario** están marcadas.
- **Eliminar acción del usuario**: la opción **Deshabilitar** está seleccionada.

  Nota Con **Deshabilitar** seleccionada, cuando los usuarios se eliminan de Active Directory, no se muestran automáticamente como "deshabilitados" en VMware Identity Services. Se trata del comportamiento esperado.

  - En Active Directory, en lugar de eliminar al usuario en el siguiente ciclo de aprovisionamiento, la propiedad del usuario pasa a ser "active"="false".
  - El usuario no aparece como "deshabilitado" en VMware Identity Services hasta que se crea o actualiza otro usuario en Active Directory en el siguiente ciclo de aprovisionamiento y se sigue la solución alternativa en https://support.pingidentity.com/s/article/After-deleting-an-AD-user-account-SaaS-provisioner-does-not-remove-the-user-in-the-next-provisioning-cycle-when-Group-DN-is-specified.

- **Origen del nombre del grupo**: la opción **Nombre común** está seleccionada.

k En la pestaña **Administrar canales**, haga clic en **Crear**.

- En la pestaña **Información del canal**:
  - **Nombre del canal**: introduzca un nombre.
  - Acepte los valores predeterminados de **Subprocesos máx.** y **Tiempo de espera (segundos)**.

l Haga clic en **Siguiente**.

- En la pestaña **Origen**:
  - **Almacén de datos activo**: elija el dominio de Active Directory.

m Haga clic en **Siguiente**.

- En la pestaña **Ubicación de origen**:
  - **DN base**: introduzca el DN base para buscar usuarios y grupos.
  - **Usuarios**: personalice en función de su entorno. Por ejemplo:
    - **DN de grupo:** no utilizar.
    - **Filtro**: introduzca `(|(objectClass=person)(objectClass=organizationalPerson)(objectClass=user))`.
  - Grupos: personalice en función de su entorno. Por ejemplo:
    - **DN de grupo**: no utilizar.
    - **Filtro**: introduzca `(objectClass=group)`.

n Haga clic en **Siguiente**.

o Acepte los valores predeterminados en la pestaña **Asignación de atributos**.

p Haga clic en **Siguiente**.

En la pestaña **Activación y resumen**:

- **Estado del canal**: seleccione **Activo**.

q Haga clic en **Listo**.

Se crea la conexión de SP y se muestra la pantalla Conexiones de SP.

r Haga clic en **Listo**.

s En la pestaña **Aprovisionamiento saliente**, haga clic en **Siguiente**.

t Revise el resumen y, luego, haga clic en **Guardar**.

u Para activar la conexión, active el control deslizante **Habilitado**.

Resultados

PingFederate ahora inserta usuarios y grupos del almacén de datos configurados a vCenter Server. Deje algún tiempo para que se produzca la inserción. Puede ver los usuarios y grupos insertados en vSphere Client. Vaya a **Administración > Inicio de sesión único > Usuarios y grupos** y seleccione el dominio PingFederate.

Pasos siguientes

Continúe con Configurar vCenter Server para la autorización de PingFederate.

Configurar vCenter Server para la autorización de PingFederate

Puede asignar usuarios de PingFederate a un grupo de vCenter Server o asignar permisos globales y de nivel de inventario a los usuarios de PingFederate.

El permiso mínimo necesario para que un usuario de PingFederate inicie sesión es de solo lectura.

Requisitos previos

Realice las siguientes tareas:

- Crear los ámbitos
- Crear una configuración común para flujos de trabajo de PingFederate
- Crear la configuración de flujo de concesión de contraseña
- Crear la configuración del flujo de código de autorización
- Instalar el aprovisionador de SCIM
- Configurar la federación de proveedores de identidad de vCenter Server para PingFederate
- Crear la aplicación de SCIM (conexión de SP)

Procedimiento

1 Para asignar usuarios de PingFederate a un grupo, consulte Agregar miembros a un grupo de vCenter Single Sign-On.

2 Para asignar permisos globales y de nivel de inventario a los usuarios de PingFederate, consulte el tema sobre la administración de permisos para los componentes de vCenter Server en la documentación de *Seguridad de vSphere*.

3 Después de asignar permisos de usuario PingFederate, compruebe que el usuario pueda iniciar sesión.

Configurar VMware Single Sign-On

Después de actualizar a vSphere 8.0 Update 3 o de instalarlo, puede configurar hosts de vCenter Server para VMware Single Sign-On. Al configurar VMware Single Sign-On, se utiliza un proveedor de identidad externo para iniciar sesión en los hosts de vCenter Server.

VMware Single Sign-On permite conectar hosts de vCenter Server en una configuración que no sea de Enhanced Linked Mode. Es decir, siempre que configure un proveedor de identidad externo, puede aprovechar esa configuración para Single Sign-On en otros hosts de vCenter Server.El host de vCenter Server en el que está configurado el proveedor de identidad externo actúa como proveedor de identidad de los otros hosts de vCenter Server.

Puede configurar varios hosts de vCenter Server para ejecutar VMware Single Sign-On. Para ello, debe configurar cada host de vCenter Server de modo que apunte al host de vCenter Server configurado con un proveedor de identidad externo.

Después de configurar VMware Single Sign-On, puede seguir iniciando sesión en los hosts de vCenter Server con una cuenta local.

Nota VMware Single Sign-On no comparte inventarios entre hosts de vCenter Server, como sucede en Enhanced Linked Mode.

Requisitos previos

Requisitos de VMware Single Sign-On:

- En la instancia de vCenter Server en la que se configura VMware Single Sign-On, se ejecuta vSphere 8.0 Update 3.
- Los hosts de vCenter Server que desee conectar para ejecutar al menos vSphere 8.0 Update 1.
- Configuró uno de los siguientes proveedores de identidad externos:
  - Microsoft Entra ID
  - Okta
  - PingFederate

- Debe agregar el certificado raíz de confianza del host de vCenter Server en el que está configurado el proveedor de identidad externo al host de vCenter Server en el que configura VMware Single Sign-On.

Procedimiento

1 Descargue el certificado raíz de confianza del host de vCenter Server en el que está configurado el proveedor de identidad externo. Por ejemplo, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2108294.

2 Cargue ese certificado raíz de confianza en el host de vCenter Server en el que va a configurar VMware SSO.

   Consulte Agregar un certificado raíz de confianza al almacén de certificados mediante vSphere Client.

3 Utilice vSphere Client para iniciar sesión como administrador en el host de vCenter Server en el que va a configurar VMware SSO.

4 Desplácese hasta **Inicio > Administración > Inicio de sesión único > Configuración**.

5 Haga clic en **Cambiar proveedor** y seleccione **VMware SSO**.

   Se abrirá el asistente **Configurar proveedor de identidad principal**.

6 En el panel **Requisitos previos**, revise los requisitos de vCenter Server.

7 Haga clic en **Ejecutar comprobaciones previas**.

   Si la comprobación previa encuentra errores, haga clic en **Ver detalles** y siga los pasos para resolver los errores como se indica.

8 Cuando se apruebe la comprobación previa, haga clic en la casilla de confirmación y, a continuación, haga clic en **Siguiente**.

9 En el panel **OpenID Connect**, introduzca la siguiente información.

   - Nombre del proveedor de identidad: se rellena con VMware SSO.
   - FQDN de vCenter Server: introduzca el FQDN del host de vCenter Server en el que está configurado el proveedor de identidad externo.
   - Número de puerto: acepte el valor predeterminado 443 o cambie al puerto que desea utilizar.
   - Nombre de usuario y contraseña: introduzca el nombre de usuario y la contraseña de una cuenta de administrador en este host de vCenter Server en el que está configurado el proveedor de identidad externo.

10 Haga clic en **Siguiente**.

11 Revise la información y haga clic en **Finalizar**.

vCenter Server crea el proveedor de identidad de VMware SSO y muestra la información de configuración. Este host de vCenter Server ahora contiene la misma configuración de proveedor de identidad externo que el host en el que se creó la configuración. Por ejemplo, cuando se comparan las configuraciones de OpenID de los dos hosts, son iguales.

12 Configure vCenter Server de modo que utilice el proveedor de identidad externo para la autorización.

Puede asignar los usuarios del proveedor de identidad externo a un grupo de vCenter Server o asignar permisos globales y de nivel de inventario a los usuarios. El permiso mínimo necesario para iniciar sesión es de solo lectura.

Para asignar los usuarios del proveedor de identidad externo a un grupo, consulte Agregar miembros a un grupo de vCenter Single Sign-On. Para asignar permisos globales y de nivel de inventario a los usuarios, consulte el tema sobre la administración de permisos para los componentes de vCenter Server en la documentación de *Seguridad de vSphere*.

13 Compruebe que se inicie sesión en este host de vCenter Server con un usuario de proveedor de identidad externo.

Al iniciar vSphere Client, verá la pantalla de bienvenida a VMware vSphere, con el botón **Iniciar sesión con SSO**. Al hacer clic en este botón, se lo redirigirá a la pantalla de inicio de sesión del proveedor de identidad externo.

Administrar VMware Identity Services

Puede detener e iniciar VMware identity Services, volver a generar un token de SCIM, y restaurar usuarios y grupos de SCIM eliminados.

Según la tarea, utilice vSphere Client o la consola de administración del proveedor de identidad externo.

Detener e iniciar VMware Identity Services

Para configurar y ejecutar Okta, Microsoft Entra ID (anteriormente Azure AD) o PingFederate como proveedor de identidad externo, se debe iniciar VMware Identity Services en vCenter Server. De forma predeterminada, al instalar o actualizar a vSphere 8.0 Update 1 o posterior, se inicia VMware Identity Services. Utilice la interfaz de administración de vCenter Server para administrar VMware Identity Services.

A partir de la versión 8.0 Update 1, vSphere incluye VMware Identity Services para tener compatibilidad con la autenticación en Okta. A partir de la versión 8.0 Update 2, VMware Identity Services admiten la autenticación con Microsoft Entra ID. A partir de la versión 8.0 Update 3, VMware Identity Services admiten la autenticación con PingFederate.

Requisitos previos

Al instalar o actualizar a vSphere 8.0 Update 1 o posterior, VMware Identity Services se inicia automáticamente. Al configurar Okta, Microsoft Entra ID o PingFederate como proveedor de identidad externo, no es necesario iniciar VMware Identity Services, ya que ya está en ejecución. Para iniciar o detener VMware Identity Services, debe ser raíz.

Configure el proveedor de identidad externo en un solo vCenter Server. Esa instancia de vCenter Server, a través de su instancia de VMware Identity Services, se comunica con el proveedor de identidad. Los otros sistemas de vCenter Server en la configuración de Enhanced Linked Mode también tienen VMware Identity Services en ejecución. Sin embargo, no se comunican directamente con el proveedor de identidad.

Procedimiento

1 En un explorador web, vaya a la interfaz de administración de vCenter Server en https://*dirección-IP-o-FQDN-de-vCenter*:5480.

2 Inicie sesión como raíz.

   La contraseña raíz predeterminada es la que estableció al implementar vCenter Server.

3 Seleccione **Servicios**

4 Vea el estado de VMware Identity Services.

5 Para detener o iniciar el servicio, seleccione **VMware Identity Services** y, a continuación, haga clic en **Detener** o **Iniciar**.

   Después de iniciar VMware Identity Services, no es necesario reiniciar vCenter Server.

Volver a generar el token de SCIM en vCenter Server

En vCenter Server, puede volver a generar un token de administración de identidades entre dominios (SCIM) para un proveedor de identidad externo.

Si genera otro token, este se activa inmediatamente y se revoca el token anterior.

Requisitos previos

Debe haber creado un proveedor de identidad externo en vCenter Server.

Procedimiento

1 Inicie sesión como administrador con vSphere Client en vCenter Server.

2 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

3 En la página **Configuración**, en **Aprovisionamiento de usuarios/Token secreto**, haga clic en **Regenerar** para volver a generar el token secreto. Seleccione la duración del token en el menú desplegable y, a continuación, haga clic en **Copiar en el portapapeles**. Guarde el token en una ubicación segura.

4 El token copiado está disponible para actualizar la configuración del proveedor de identidad externo.

Restaurar usuarios y grupos de SCIM eliminados

Si los usuarios y grupos insertados desde SCIM de la instancia de vCenter Server no están sincronizados con el proveedor de identidad externo, puede realizar los pasos necesarios para solucionar el problema.

Cuando desee restaurar un usuario o un grupo insertado desde SCIM que eliminó de vCenter Server, no puede simplemente insertar el usuario o el grupo desde el proveedor de identidad. Debido a la forma en que vCenter Server utiliza el sistema para la administración de identidades entre dominios (SCIM) para la administración de usuarios y grupos, debe actualizar la propia aplicación SCIM 2.0 con el usuario o el grupo faltantes.

Procedimiento

1 Inicie sesión en la consola administrativa de IDP externo.

2 Desplácese hasta la aplicación SCIM 2.0.

3 Asigne el usuario o grupo eliminado o faltante.

4 Seleccione la acción adecuada para eliminar el usuario o grupo insertado para desvincular el grupo o el usuario insertados.

5 Seleccione la acción adecuada para insertar el grupo.

6 Compruebe en vCenter Server que el IDP externo haya sincronizado el grupo o el usuario.

vCenter Single Sign-On

Si no utiliza un proveedor de identidad externo, debe comprender la arquitectura subyacente del proveedor de identidad integrado, vCenter Single Sign-On y cómo afecta a la instalación y las actualizaciones.

Componentes de vCenter Single Sign-On

vCenter Single Sign-On incluye el servicio de token de seguridad (STS), un servidor de administración, vCenter Lookup Service y VMware Directory Service (vmdir). VMware Directory Service también se usa para la administración de certificados.

Durante la instalación, los siguientes componentes se implementan como parte de una implementación de vCenter Server.

STS (servicio de token de seguridad)

El servicio STS emite tokens de lenguaje de marcado de aserción de seguridad (Security Assertion Markup Language, SAML). Estos tokens de seguridad representan la identidad de un usuario en uno de los tipos de orígenes de identidad compatibles con vCenter Server. Los tokens de SAML permiten que los usuarios interactivo, de script y de servicio (incluidos los usuarios de soluciones) que se autentican correctamente en vCenter Single Sign-On utilicen cualquier servicio de vCenter que sea compatible con vCenter Single Sign-On sin tener que volver a autenticarse en cada servicio.

El servicio vCenter Single Sign-On firma todos los tokens con un certificado de firma y almacena el certificado de firma de tokens en el disco. El certificado del propio servicio también se almacena en el disco.

Servidor de administración

El servidor de administración permite que los usuarios con privilegios de administrador para vCenter Single Sign-On configuren el servidor vCenter Single Sign-On y administren usuarios y grupos de vSphere Client. Inicialmente, solo el usuario administrator@*su_nombre_de_dominio* tenía estos privilegios. Puede cambiar el dominio de vSphere al instalar vCenter Server. No asigne el nombre de dominio de Microsoft Active Directory u OpenLDAP a su nombre de dominio.

VMware Directory Service (vmdir)

VMware Directory Service (vmdir) se asocia al dominio que especifique durante la instalación y se incluye en cada implementación de vCenter Server. Se trata de un servicio de directorio multiempresa y de replicación de elementos del mismo nivel que pone a disposición un directorio LDAP en el puerto 389. También almacena y administra las cuentas de usuario y las contraseñas de vCenter Single Sign-On, que están protegidas por el algoritmo de hash SHA-512.

Si su entorno incluye varias instancias de vCenter Server configuradas en el modo vinculado, se propaga una actualización del contenido de vmdir de una instancia de vmdir a todas las demás.

VMware Directory Service no solo almacena información de vCenter Single Sign-On, sino también información de certificado.

Servicio de administración de identidades

Controla los orígenes de identidad y las solicitudes de autenticación de STS.

Usar vCenter Single Sign-On con vSphere

vCenter Single Sign-On lleva a cabo una autenticación cuando un usuario inicia sesión en un componente de vSphere o cuando un usuario de una solución de vCenter Server accede a otro servicio de vCenter Server. Los usuarios deben autenticarse con vCenter Single Sign-On y tener los privilegios necesarios para interactuar con objetos de vSphere.

vCenter Single Sign-On autentica a los usuarios de solución y a otros usuarios.

- Los usuarios de solución representan un conjunto de servicios en el entorno de vSphere. Durante la instalación, VMCA asigna un certificado a cada usuario de solución de forma predeterminada. El usuario de solución utiliza ese certificado para autenticarse ante vCenter Single Sign-On. vCenter Single Sign-On proporciona un token SAML al usuario de solución y, a continuación, el usuario de la solución puede interactuar con otros servicios del entorno.
- Cuando otros usuarios inician sesión en el entorno, por ejemplo, desde vSphere Client, vCenter Single Sign-On solicita un nombre de usuario y una contraseña. Si vCenter Single Sign-On encuentra un usuario con esas credenciales en el origen de identidad correspondiente, le asigna un token SAML. De esta forma, el usuario puede acceder a otros servicios del entorno sin tener que autenticarse de nuevo.

  Los objetos que el usuario puede ver y lo que este puede hacer están determinados por los parámetros de configuración de permiso de vCenter Server. Los administradores de vCenter Server asignan esos permisos desde la interfaz **Permisos** en vSphere Client, o a través de vCenter Single Sign-On. Consulte la documentación de *Seguridad de vSphere*.

Usuarios de vCenter Single Sign-On y vCenter Server

Los usuarios se autentican en vCenter Single Sign-On introduciendo sus credenciales en la página de inicio de sesión. Después de conectarse a vCenter Server, los usuarios autenticados pueden ver todas las instancias de vCenter Server u otros objetos de vSphere para los que su función les da privilegios. En esta instancia ya no se requiere autenticación adicional.

Después de la instalación, el administrador del dominio de vCenter Single Sign-On, administrator@vsphere.local de manera predeterminada, tiene acceso de administrador tanto a vCenter Single Sign-On como a vCenter Server. Ese usuario puede agregar orígenes de identidad, establecer el origen de identidad predeterminado y administrar usuarios y grupos en el dominio de vCenter Single Sign-On.

Todos los usuarios que pueden autenticarse en vCenter Single Sign-On pueden restablecer su contraseña. Consulte Cambiar la contraseña de vCenter Single Sign-On . Solo los administradores de vCenter Single Sign-On pueden restablecer la contraseña de los usuarios que ya no tienen su contraseña.

Usuarios administradores de vCenter Single Sign-On

El acceso a la interfaz de administración de vCenter Single Sign-On se realiza desde vSphere Client.

Para configurar vCenter Single Sign-On y administrar usuarios y grupos de vCenter Single Sign-On, el usuario administrator@vsphere.local o un usuario del grupo de administradores de vCenter Single Sign-On deben iniciar sesión en vSphere Client. Después de la autenticación, el usuario puede acceder a la interfaz de administración de vCenter Single Sign-On desde vSphere Client y administrar orígenes de identidad y dominios predeterminados, especificar directivas de contraseñas y realizar otras tareas administrativas.

Nota No puede cambiar el nombre de usuario administrador de vCenter Single Sign-On, que es administrator@vsphere.local de manera predeterminada o administrator@*mydomain* si especificó un dominio diferente durante la instalación. Para mejorar la seguridad, se recomienda que cree usuarios designados adicionales en el dominio vCenter Single Sign-On y les asigne privilegios administrativos. Luego puede dejar de usar la cuenta de administrador.

Otras cuentas de usuario en vCenter Server

Las siguientes cuentas de usuario se crean automáticamente en vCenter Server en el dominio vsphere.local (o en el dominio predeterminado que creó durante la instalación). Estas cuentas de usuario son cuentas de shell. La directiva de contraseñas de vCenter Single Sign-On no se aplica a estas cuentas.

Tabla 4-1. Otras cuentas de usuario de vCenter Server

Cuenta	Descripción
K/M	Para la administración de claves de Kerberos.
krbtgt/VSPHERE.LOCAL	Para la compatibilidad con la autenticación integrada de Windows.
waiter-*random_string*	Para Auto Deploy.

Usuarios de ESXi

Los hosts ESXi independientes no están integrados con vCenter Single Sign-On. Consulte *Seguridad de vSphere* para obtener información sobre cómo agregar un host ESXi a Active Directory.

Si se crean usuarios de ESXi locales para un host ESXi administrado con VMware Host Client, ESXCLI o PowerCLI, vCenter Server no sabe quiénes son esos usuarios. Por ello, la creación de usuarios locales puede derivar en confusión, especialmente si usa los mismos nombres de usuario. Los usuarios que pueden autenticar en vCenter Single Sign-On pueden ver y administrar hosts ESXi si tienen los permisos correspondiente en el objeto de host ESXi.

Nota De ser posible, administre los permisos de hosts ESXi mediante vCenter Server.

Cómo iniciar sesión en componentes de vCenter Server

Puede iniciar sesión conectándose a vSphere Client.

Cuando un usuario inicia sesión en un sistema vCenter Server desde vSphere Client, el comportamiento de inicio de sesión depende de si el usuario se encuentra o no en el dominio configurado como el origen de identidad predeterminado.

- Los usuarios que están en el dominio predeterminado pueden iniciar sesión con su nombre de usuario y contraseña.
- Los usuarios que están en un dominio que se ha agregado a vCenter Single Sign-On como un origen de identidad, pero que no es el dominio predeterminado, pueden iniciar sesión en vCenter Server, pero deben especificar el dominio de una de las siguientes maneras.
  - Incluyendo un prefijo de nombre de dominio; por ejemplo, MIDOMINIO\usuario1.
  - Incluyendo el dominio; por ejemplo, usuario1@midominio.com.
- Los usuarios que se encuentran en un dominio que no es un origen de identidad de vCenter Single Sign-On no pueden iniciar sesión en vCenter Server. Si el dominio que va a agregar a vCenter Single Sign-On forma parte de una jerarquía de dominios, Active Directory determinará si los usuarios de otros dominios de la jerarquía se autentican o no.

Si el entorno incluye una jerarquía de Active Directory, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2064250 para obtener detalles sobre las configuraciones compatibles y no compatibles.

Grupos del dominio de vCenter Single Sign-On

El dominio de vCenter Single Sign-On (vsphere.local de forma predeterminada) incluye varios grupos predefinidos. Agregue usuarios a uno de esos grupos para permitirles realizar las acciones correspondientes.

Consulte Administrar usuarios y grupos de vCenter Single Sign-On.

Para todos los objetos de la jerarquía de vCenter Server, puede asignar los permisos mediante el emparejamiento de un usuario y una función con el objeto. Por ejemplo, puede seleccionar un grupo de recursos y otorgar a un grupo de usuarios la función correspondiente para proporcionarle privilegios de lectura en ese objeto del grupo de recursos.

Para algunos servicios que vCenter Server no administra directamente, los privilegios se determinan por la pertenencia a uno de los grupos de vCenter Single Sign-On. Por ejemplo, un usuario que es miembro del grupo Administradores puede administrar vCenter Single Sign-On. Un usuario miembro del grupo Administradores de CA puede administrar VMware Certificate Authority y un usuario que está en el grupo Servicio de licencias.Administradores puede administrar licencias.

Los siguientes grupos están predefinidos en vsphere.local. Muchos de estos grupos son internos de vsphere.local u otorgan a los usuarios privilegios administrativos de alto nivel. Evalúe detenidamente los riesgos antes de agregar usuarios a cualquiera de estos grupos.

Precaución No elimine ninguno de los grupos predefinidos en el dominio vsphere.local. De lo contrario, se pueden producir errores en la autenticación o el aprovisionamiento de certificados.

Tabla 4-2. Grupos del dominio vsphere.local

Privilegio	Descripción
Usuarios	Usuarios del dominio de vCenter Single Sign-On (vsphere.local de forma predeterminada).
Usuarios de solución	Grupo de usuarios de solución para los servicios de vCenter. Cada usuario de solución se autentica de forma individual en vCenter Single Sign-On con un certificado. De forma predeterminada, VMCA aprovisiona a los usuarios de solución con certificados. No agregue miembros a este grupo explícitamente.
Administradores de CA	Miembros del grupo Administradores de CA que tienen privilegios de administrador para VMCA. No agregue miembros a este grupo a menos que tenga razones de peso para hacerlo.
Administradores de DC	Los miembros del grupo Administradores de DC pueden llevar a cabo acciones de administrador de la controladora de dominio en VMware Directory Service. **Nota** No administre la controladora de dominio directamente. En su lugar, utilice la CLI `vmdir` o vSphere Client para llevar a cabo las tareas correspondientes.
Configuración del sistema.Administradores de shell de Bash	Un usuario de este grupo tiene acceso completo a todas las API de administración de dispositivos. De forma predeterminada, un usuario que se conecta a vCenter Server con SSH solo puede acceder a los comandos del shell restringido, pero los usuarios de este grupo tienen acceso al shell de Bash a través de SSH y obtienen privilegios completos similares al usuario raíz.
Actuar como usuarios	Los miembros del grupo Actuar como usuarios tienen permisos de obtención de tokens Actuar como de vCenter Single Sign-On.
ExternalIDPUsers	Este grupo interno no se utiliza en vSphere. VMware vCloud Air necesita este grupo.
Configuración del sistema.Administradores	Los miembros del grupo SystemConfiguration.Administrators pueden ver y administrar la configuración del sistema en la interfaz de administración de vCenter Server que se ejecuta en el puerto 5480. Estos usuarios pueden ver, iniciar y reiniciar servicios, y solucionar problemas con los servicios. Estos usuarios también pueden acceder a las API de administración de dispositivos, excepto las API que modifican configuraciones críticas del sistema.
Clientes de DC	Este grupo se utiliza internamente para permitir al nodo de administración acceder a los datos de VMware Directory Service. **Nota** No modifique este grupo. Cualquier cambio puede comprometer la infraestructura de certificados.

Tabla 4-2. Grupos del dominio vsphere.local (continuación)

Privilegio	Descripción
Administrador de componentes.Administradores	Los miembros del grupo Administrador de componentes.Administradores pueden ejecutar las API del administrador de componentes que registran servicios o cancelan registros de servicios, es decir, pueden modificar servicios. No es necesario ser miembro de este grupo para tener acceso de lectura en los servicios.
Servicio de licencias.Administradores	Los miembros de Servicio de licencias.Administradores tienen acceso total de escritura a todos los datos relacionados con la concesión de licencias, y pueden agregar, quitar y asignar claves de serie, así como anular estas asignaciones, para todos los activos de productos registrados en el servicio de concesión de licencias.
Administradores	Administradores de VMware Directory Service (vmdir). Los miembros de este grupo pueden realizar tareas de administración de vCenter Single Sign-On. No agregue miembros a este grupo a menos que tenga razones de peso para hacerlo y sepa cuáles son las consecuencias.
TrustedAdmins	Los miembros de este grupo pueden realizar tareas de configuración y administración de VMware® vSphere Trust Authority™. De forma predeterminada, este grupo no contiene ningún miembro. Debe agregar un miembro a este grupo para poder realizar tareas de vSphere Trust Authority.
AutoUpdate	Este grupo se utiliza de forma interna con la puerta de enlace de vCenter Cloud.
SyncUsers	Este grupo se utiliza de forma interna con la puerta de enlace de vCenter Cloud.
vSphereClientSolutionUsers	Este grupo se utiliza internamente con vSphere Client.
ServiceProviderUsers	Los miembros de este grupo pueden administrar la infraestructura de vSphere with Tanzu y VMware Cloud on AWS.
NsxAdministrators	Este grupo se utiliza para VMware NSX.
WorkloadStorage	Grupo de almacenamiento de carga de trabajo.
RegistryAdministrators	Los miembros de este grupo pueden administrar el registro.
NsxAuditors	Este grupo se utiliza para VMware NSX.
NsxViAdministrators	Este grupo se utiliza para VMware NSX.
SystemConfiguration.SupportUsers	Los miembros del grupo SystemConfiguration.SupportUsers pueden acceder a la API del paquete de soporte.
SystemConfiguration.ReadOnly	Los miembros de este grupo pueden acceder a operaciones de solo lectura de vCenter Server Appliance en Administración de dispositivos.

Tabla 4-2. Grupos del dominio vsphere.local (continuación)

Privilegio	Descripción
VCLSAdmin	Los miembros de este grupo tienen privilegios administrativos para vSphere Cluster Services (vCLS).
AnalyticsService.Administrators	Este grupo se utiliza para las API de VMware Analytics Service.
vStatsGroup	Este grupo se utiliza para la recopilación de vStats.

Configurar orígenes de identidad de vCenter Single Sign-On

Cuando un usuario inicia sesión solo con un nombre de usuario, vCenter Single Sign-On comprueba en el origen de identidad predeterminado si ese usuario puede autenticarse. Cuando un usuario inicia sesión e incluye el nombre de dominio en la pantalla de inicio de sesión, vCenter Single Sign-On comprueba el dominio especificado si ese dominio se agregó como origen de identidad. Es posible agregar orígenes de identidad, quitar orígenes de identidad y cambiar el valor predeterminado.

vCenter Single Sign-On se configura desde vSphere Client. Para configurar vCenter Single Sign-On, se deben tener privilegios de administrador de vCenter Single Sign-On. Tener privilegios de administrador de vCenter Single Sign-On es diferente a tener función de administrador en vCenter Server o ESXi. En una nueva instalación, solo el administrador de vCenter Single Sign-On (administrator@vsphere.local de forma predeterminada) puede autenticarse en vCenter Single Sign-On.

Orígenes de identidad para vCenter Server con vCenter Single Sign-On

Puede utilizar orígenes de identidad para adjuntar uno o más dominios a vCenter Single Sign-On. Un dominio es un repositorio para usuarios y grupos que el servidor vCenter Single Sign-On puede utilizar para autenticación de usuarios.

Nota En vSphere 7.0 Update 2 y versiones posteriores, puede habilitar FIPS en vCenter Server. Consulte la documentación de *Seguridad de vSphere*. AD en LDAP no se admite cuando FIPS está habilitado. Utilice la federación de proveedores de identidad externos en modo FIPS. Consulte Configurar la federación de proveedores de identidad de vCenter Server.

Los administradores pueden agregar orígenes de identidad, configurar el origen de identidad predeterminado y crear usuarios y grupos en el origen de identidad vsphere.local.

Los datos de usuarios y grupos se almacenan en Active Directory, OpenLDAP o localmente en el sistema operativo del equipo en el que está instalado vCenter Single Sign-On. Después de la instalación, cada instancia de vCenter Single Sign-On tiene el origen de identidad *your_domain_name*, por ejemplo vsphere.local. Este origen de identidad es interno para vCenter Single Sign-On.

Nota En todo momento, solo hay un único dominio predeterminado. Si un usuario de un dominio que no es el predeterminado inicia sesión, debe agregar el nombre de dominio para poder autenticarse correctamente. El nombre de dominio tiene el siguiente formato:

```
DOMAIN\user
```

Los siguientes orígenes de identidad están disponibles.

- Active Directory a través de LDAP. vCenter Single Sign-On admite varios orígenes de identidad de Active Directory en LDAP.
- Active Directory (autenticación de Windows integrada), versiones 2003 y posteriores. vCenter Single Sign-On permite especificar un único dominio de Active Directory como origen de identidad. El dominio puede tener dominios secundarios o ser un dominio raíz del bosque. En el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2064250 se analiza las confianzas de Microsoft Active Directory compatibles con vCenter Single Sign-On.
- Versiones de OpenLDAP 2.4 y posteriores. vCenter Single Sign-On admite varios orígenes de identidad de OpenLDAP.

Nota Una actualización de Microsoft Windows cambió el comportamiento predeterminado de Active Directory para exigir una autenticación y un cifrado seguros. Este cambio afecta el modo en que vCenter Server se autentica en Active Directory. Si utiliza Active Directory como origen de identidad para vCenter Server, debe habilitar LDAPS. Para obtener más información, consulte https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 y https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Establecer el dominio predeterminado de vCenter Single Sign-On

Cada origen de identidad de vCenter Single Sign-On está asociado a un dominio. vCenter Single Sign-On utiliza el dominio predeterminado para autenticar a un usuario que inicia sesión sin un nombre de dominio. Los usuarios que pertenecen a un dominio que no es el predeterminado deben incluir el nombre de dominio para iniciar sesión.

Cuando un usuario inicia sesión en un sistema vCenter Server desde vSphere Client, el comportamiento de inicio de sesión depende de si el usuario se encuentra o no en el dominio configurado como el origen de identidad predeterminado.

- Los usuarios que están en el dominio predeterminado pueden iniciar sesión con su nombre de usuario y contraseña.

- Los usuarios que están en un dominio que se ha agregado a vCenter Single Sign-On como un origen de identidad, pero que no es el dominio predeterminado, pueden iniciar sesión en vCenter Server, pero deben especificar el dominio de una de las siguientes maneras.
  - Incluyendo un prefijo de nombre de dominio; por ejemplo, MIDOMINIO\usuario1.
  - Incluyendo el dominio; por ejemplo, usuario1@midominio.com.
- Los usuarios que se encuentran en un dominio que no es un origen de identidad de vCenter Single Sign-On no pueden iniciar sesión en vCenter Server. Si el dominio que va a agregar a vCenter Single Sign-On forma parte de una jerarquía de dominios, Active Directory determinará si los usuarios de otros dominios de la jerarquía se autentican o no.

Procedimiento

1. Inicie sesión con vSphere Client en vCenter Server.
2. Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.
3. Desplácese hasta la interfaz de usuario de configuración.
   a. En el menú **Inicio**, seleccione **Administración**.
   b. En **Single Sign On**, haga clic en **Configuración**.
4. En la pestaña **Proveedor de identidad**, haga clic en **Orígenes de identidad**, seleccione un origen de identidad y haga clic en **Establecer como predeterminado**.
5. Haga clic en **Aceptar**.

   En la pantalla del dominio, el dominio predeterminado muestra la opción (predeterminado) en la columna Tipo.

Agregar o editar un origen de identidad vCenter Single Sign-On

Los usuarios pueden iniciar sesión en vCenter Server solo si están en un dominio que se agregó como origen de identidad de vCenter Single Sign-On. Los usuarios administradores de vCenter Single Sign-On pueden agregar orígenes de identidad o cambiar la configuración de los orígenes de identidad que agregaron.

Un origen de identidad puede ser un dominio de Active Directory en LDAP, un dominio nativo de Active Directory (autenticación integrada de Windows) o un servicio de directorio de OpenLDAP. Consulte Orígenes de identidad para vCenter Server con vCenter Single Sign-On.

Inmediatamente después de la instalación, está disponible el dominio vsphere.local (o el dominio que especificó durante la instalación) con los usuarios internos de vCenter Single Sign-On.

Nota Si actualizó o reemplazó el certificado SSL de Active Directory, debe eliminar y volver a agregar el origen de identidad en vCenter Server.

Requisitos previos

Si va a agregar un origen de identidad de Active Directory (autenticación integrada de Windows), vCenter Server debe estar en el dominio de Active Directory. Consulte Agregar una instancia de vCenter Server a un dominio de Active Directory.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 En la pestaña **Proveedor de identidad**, haga clic en **Orígenes de identidad** y, a continuación, en **Agregar**.

5 Seleccione el origen de identidad e introduzca su configuración.

Opción	Descripción
Active Directory (autenticación integrada de Windows)	Utilice esta opción para las implementaciones nativas de Active Directory. Si desea utilizar esta opción, la máquina en la que se ejecuta el servicio vCenter Single Sign-On debe estar en un dominio de Active Directory. Consulte Configurar orígenes de identidad de Active Directory.
Active Directory en LDAP	Esta opción requiere que especifique el controlador de dominio y otra información. Consulte Configurar orígenes de identidad de servidores OpenLDAP y Active Directory en LDAP.
OpenLDAP	Utilice esta opción para un origen de identidad OpenLDAP. Consulte Configurar orígenes de identidad de servidores OpenLDAP y Active Directory en LDAP.

   Nota Si se bloquea o se desactiva la cuenta, las autenticaciones y las búsquedas de grupos y de usuarios en el dominio de Active Directory no funcionan. La cuenta del usuario debe tener acceso de solo lectura a la unidad organizativa del usuario y del grupo, y debe poder leer los atributos del usuario y del grupo. Active Directory ofrece este acceso de manera predeterminada. Utilice un usuario de servicio especial para obtener una mayor seguridad.

6 Haga clic en **Agregar**.

Pasos siguientes

Al principio, se asigna la función Sin acceso a cada usuario. Un administrador de vCenter Server debe asignar al menos la función Solo lectura al usuario para que pueda iniciar sesión. Consulte el tema sobre el uso de funciones para asignar privilegios en la documentación de *Seguridad de vSphere*.

Configurar orígenes de identidad de servidores OpenLDAP y Active Directory en LDAP

El origen de identidad de Active Directory en LDAP es preferible a la opción de Active Directory (autenticación de Windows integrada). El origen de identidad de servidores OpenLDAP está disponible para los entornos que usan OpenLDAP.

Si planea configurar un origen de identidad de OpenLDAP, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2064977 para ver los requisitos adicionales.

Importante Los grupos de orígenes de identidad de AD sobre LDAP no pueden utilizar usuarios en diferentes dominios, incluso si se crea un origen de identidad adicional para cada dominio.

Los grupos de orígenes de identidad de LDAP solo reconocen a los usuarios que existen en el DN base de usuarios especificado. Esto puede provocar problemas inesperados en entornos grandes de Active Directory con dominios secundarios. Por ejemplo, supongamos el siguiente escenario:

1 Un bosque de Active Directory con dos dominios secundarios: ChildA y ChildB.

2 Una instancia de vCenter Server configurada con dos orígenes de identidad de AD sobre LDAP, uno para el dominio secundario ChildA y otro para el dominio secundario ChildB.

3 ChildA contiene dos usuarios denominados UserA1 y UserA2.

4 ChildB contiene dos usuarios denominados UserB1 y UserB2.

El administrador de vCenter Server crea un grupo en ChildA denominado TestGroup que contiene UserA1, UserA2, UserB1 y UserB2. El administrador de vCenter Server concede privilegios de inicio de sesión (o cualquiera) a TestGroup. Lamentablemente, UserB1 y UserB2 no pueden iniciar sesión porque residen en un dominio diferente al del grupo.

Como solución alternativa, haga lo siguiente:

1 Cree otro grupo denominado SecondTestGroup en ChildB.

2 Elimine UserB1 y UserB2 de TestGroup.

3 Agregue UserB1 y UserB2 a SecondTestGroup.

4 En vCenter Server, asigne a SecondTestGroup los mismos privilegios que se concedieron a TestGroup.

Nota Microsoft Windows cambió el comportamiento predeterminado de Active Directory para exigir una autenticación y un cifrado seguros. Este cambio afecta el modo en que vCenter Server se autentica en Active Directory. Si utiliza Active Directory como origen de identidad para vCenter Server, debe habilitar LDAPS. Para obtener más información sobre esta actualización de seguridad de Microsoft, consulte https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 y https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Tabla 4-3. Configuración de orígenes de servidores OpenLDAP y Active Directory en LDAP

Opción	Descripción
Nombre	Nombre del origen de identidad.
DN base para usuarios	El nombre distintivo base para los usuarios. Introduzca el DN desde el que se iniciarán las búsquedas de usuarios. Por ejemplo, cn=Users,dc=myCorp,dc=com.
DN base para grupos	El nombre distintivo base de los grupos. Introduzca el DN a partir del que se iniciarán las búsquedas de grupos. Por ejemplo, cn=Groups,dc=myCorp,dc=com.
Nombre de dominio	El nombre de dominio completo.
Alias de dominio	Para los orígenes de identidad de Active Directory, el nombre de NetBIOS del dominio. Si usa autenticaciones de SSPI, agregue el nombre de NetBIOS del dominio de Active Directory como alias del origen de identidad. Para los orígenes de identidad de OpenLDAP, si no se especifica un alias, se agrega el nombre del dominio en mayúsculas.
Nombre de usuario	Identificador de un usuario del dominio que tiene, como mínimo, acceso de solo lectura al DN base para los usuarios y los grupos. El identificador puede tener cualquiera de estos formatos: ■ UPN (usuario@dominio.com) ■ NetBIOS (DOMINIO\usuario) ■ DN (cn=usuario,cn=Usuarios,dc=dominio,dc=com) El nombre de usuario debe ser completo. Una entrada de "usuario" no funciona.
Contraseña	Contraseña del usuario especificado en el campo **Nombre de usuario**.
Conectar con	Controladora de dominio a la cual conectarse. Puede ser cualquier controladora de dominio en el dominio o controladoras específicas.
URL de servidor principal	El servidor LDAP de la controladora de dominio principal para el dominio. Puede utilizar el nombre de host o la dirección IP. Use el formato **`ldap://nombre de host o dirección IP:puerto`** o **`ldaps://nombre de host o dirección IP:puerto`**. Por lo general, el puerto es el 389 para las conexiones de LDAP y 636 para las conexiones de LDAPS. Para las implementaciones de controladoras de varios dominios de Active Directory, el puerto suele ser el 3268 para las conexiones de LDAP y el 3269 para las conexiones de LDAPS. Se necesita un certificado que establezca la confianza para el endpoint de LDAPS del servidor Active Directory cuando se usa **`ldaps://`** en la dirección URL del servidor LDAP principal o secundario.

Tabla 4-3. Configuración de orígenes de servidores OpenLDAP y Active Directory en LDAP (continuación)

Opción	Descripción
URL de servidor secundario	Dirección de un servidor LDAP del controlador de dominio secundario que se utiliza cuando el controlador de dominio principal no está disponible. Puede utilizar el nombre de host o la dirección IP. Para cada operación LDAP, vCenter Server siempre prueba con el controlador de dominio principal antes de conmutar por recuperación al controlador de dominio secundario. Esto puede provocar que los inicios de sesión de Active Directory tarden más tiempo e incluso generen errores cuando el controlador de dominio principal no está disponible. **Nota** Cuando se produce un error en el controlador de dominio principal, es posible que el controlador de dominio secundario no asuma la función automáticamente.
Certificados (para LDAPS)	Si desea utilizar LDAPS con su origen de identidad de servidor Active Directory LDAP o servidor OpenLDAP, haga clic en **`Navegar`** para seleccionar un certificado que se exportó del controlador de dominio especificado en la URL de LDAPS. (Tenga en cuenta que el certificado utilizado aquí no es un certificado de CA raíz). Para exportar el certificado de Active Directory, consulte la documentación de Microsoft. Puede buscar y seleccionar varios certificados. **Sugerencia** Al buscar y seleccionar varios certificados, estos deben encontrarse en el mismo directorio. vCenter Server solo confía en certificados que estén firmados directamente por una entidad de certificación registrada y de confianza. vCenter Server no rastrea una ruta de acceso hasta un certificado de CA registrada y solo comprueba si el certificado está firmado por una entidad de certificación registrada y de confianza. Siempre que el certificado esté firmado por una entidad de certificación de confianza pública o esté autofirmado, no es necesario realizar ninguna otra acción. Sin embargo, si crea sus propios certificados internos (es decir, utiliza una entidad de certificación privada), es posible que deba incluir esos certificados. Por ejemplo, si su organización utiliza una entidad de certificación raíz empresarial de Microsoft para generar el certificado LDAPS, también debe seleccionar el certificado raíz empresarial para agregarlo a vCenter Server. Asimismo, si utiliza entidades de certificación intermedias entre el certificado LDAPS y el certificado raíz empresarial, también debe seleccionar esos certificados intermedios para agregarlos a vCenter Server.

Configurar orígenes de identidad de Active Directory

Si selecciona el tipo de origen de identidad de Active Directory (autenticación integrada de Windows), puede usar la cuenta de equipo local como un nombre de entidad de seguridad de servicio (Service Principal Name, SPN) o especificar un SPN explícitamente. Puede usar esta opción únicamente si el servidor vCenter Single Sign-On está asociado a un dominio de Active Directory.

Requisitos previos para el uso de un origen de identidad de Active Directory (autenticación integrada de Windows)

Puede configurar vCenter Single Sign-On para que use un origen de identidad de Active Directory (autenticación integrada de Windows) solo si ese origen de identidad está disponible. Siga las instrucciones en la documentación de *Configuración de vCenter Server*.

Nota Active Directory (autenticación integrada de Windows) usa siempre la raíz del bosque de dominios de Active Directory. Para configurar un origen de identidad para Autenticación integrada de Windows con un dominio secundario dentro del bosque de Active Directory, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2070433.

Seleccione **Usar cuenta de equipo** para acelerar la configuración. Si desea cambiar el nombre del equipo local en el que se ejecuta vCenter Single Sign-On, es preferible que especifique un SPN explícitamente.

Si habilitó el registro de eventos de diagnóstico en Active Directory para identificar dónde es posible que se necesite una protección, puede que vea un evento de registro con el identificador 2889 en ese servidor de directorio. El identificador de evento 2889 se genera como una anomalía en lugar de un riesgo de seguridad cuando se utiliza la autenticación integrada de Windows. Para obtener más información sobre el identificador de evento 2889, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/78644.

Tabla 4-4. Agregar opciones de orígenes de identidad

Cuadro de texto	Descripción
Nombre de dominio	FQDN del nombre de dominio (por ejemplo, midominio.com). No incluya una dirección IP. El sistema vCenter Server debe poder resolver este nombre de dominio mediante DNS.
Usar cuenta de equipo	Seleccione esta opción para usar la cuenta de equipo local como el SPN. Si selecciona esta opción, solo debe especificar el nombre de dominio. No seleccione esta opción si desea cambiar el nombre de este equipo.
Usar nombre de entidad de seguridad de servicio (SPN)	Seleccione esta opción si desea cambiar el nombre del equipo local. Debe especificar un SPN, un usuario que pueda autenticarse con el origen de identidad y una contraseña para el usuario.

Tabla 4-4. Agregar opciones de orígenes de identidad (continuación)

Cuadro de texto	Descripción
Nombre de entidad de seguridad de servicio (SPN)	SPN ayuda a que Kerberos identifique el servicio de Active Directory. Incluya un dominio en el nombre (por ejemplo, `STS/ejemplo.com`). El SPN debe ser único en todo el dominio. La ejecución de `setspn -S` comprueba que no se creen duplicados. Consulte la documentación de Microsoft para obtener información sobre `setspn`.
Nombre principal de usuario (UPN) **Contraseña**	Nombre y contraseña de un usuario que puede autenticarse con este origen de identidad. Utilice el formato de dirección de correo electrónico (por ejemplo, `jchin@midominio.com`). Puede comprobar el nombre principal de usuario con el editor de interfaces del servicio de Active Directory (editor ADSI).

Agregar o quitar un origen de identidad mediante la CLI

Puede usar la utilidad `sso-config` para agregar o quitar un origen de identidad.

Un origen de identidad puede ser un dominio nativo de Active Directory (autenticación integrada de Windows), AD over LDAP, AD over LDAP using LDAPS (LDAP over SSL) u OpenLDAP. Consulte Orígenes de identidad para vCenter Server con vCenter Single Sign-On. También puede utilizar la utilidad `sso-config` para configurar la autenticación de tarjeta inteligente y de RSA SecurID.

Requisitos previos

Si va a agregar un origen de identidad de Active Directory, vCenter Server debe estar en el dominio de Active Directory. Consulte Agregar una instancia de vCenter Server a un dominio de Active Directory.

Habilite el inicio de sesión en SSH. Consulte Administrar vCenter Server mediante el shell de vCenter Server.

Procedimiento

1 Utilice SSH u otra conexión de consola remota para iniciar una sesión en el sistema de vCenter Server.

2 Inicie sesión como raíz.

3 Pase al directorio donde se ubica la utilidad `sso-config`.

```
cd /opt/vmware/bin
```

4 Para consultar la ayuda de `sso-config`, ejecute `sso-config.sh -help` o vea el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/67304 para obtener ejemplos de uso.

Administrar el servicio de token de seguridad de vCenter Server

El servicio de token de seguridad (STS) de vCenter Server es un servicio web que emite, valida y renueva los tokens de seguridad.

Como emisor de tokens, el servicio de token de seguridad (STS) utiliza una clave privada para firmar tokens y publica los certificados públicos para que los servicios puedan comprobar la firma del token. vCenter Server administra los certificados de firma de STS y los almacena en VMware Directory Service (vmdir). Los tokens pueden tener una duración considerable e, históricamente, podrían haber sido firmados por diversas claves.

Los usuarios presentan sus credenciales principales a la interfaz de STS para adquirir los tokens. La credencial principal depende del tipo de usuario.

Tabla 4-5. Usuarios y credenciales de STS

Tipo de usuario	Credenciales primarias
Usuario de solución	Certificado válido.
Otros usuarios	Nombre de usuario y contraseña disponibles en un origen de identidad de vCenter Single Sign-On.

El STS autentica al usuario en función de las credenciales principales y crea un token SAML que contiene los atributos del usuario.

De forma predeterminada, VMware Certificate Authority (VMCA) genera el certificado de firma de STS. Puede actualizar el certificado de firma de STS con un nuevo certificado de VMCA. También puede importar y reemplazar el certificado de firma de STS predeterminado por un certificado de firma de STS personalizado o generado por terceros. No reemplace el certificado de firma STS a menos que la directiva de seguridad de la empresa exija que se reemplacen todos los certificados.

Puede utilizar el vSphere Client para:

- Actualizar certificados de STS
- Importar y reemplazar certificados STS personalizados y generados por terceros
- Ver detalles del certificado STS, como la fecha de caducidad

También puede utilizar la línea de comandos para reemplazar certificados STS personalizados y generados por terceros.

Duración y caducidad del certificado STS

Una instalación nueva de vSphere 7.0 Update 1 y posterior crea un certificado de firma de STS con una duración de 10 años. Cuando un certificado de firma de STS está a punto de caducar, una alarma le advierte empezando a los 90 días una vez por semana y, a continuación, a diario cuando quedan siete días.

Nota En determinadas circunstancias, reemplazar los certificados de firma de STS puede cambiar la duración de los certificados. Al reemplazar certificados, preste atención a las fechas de emisión y caducidad.

Renovación automática del certificado STS

En vSphere 8.0 y versiones posteriores, vCenter Single Sign-On renueva automáticamente un certificado de firma del servicio de token de seguridad (STS, Security Token Service) generado por VMCA. La renovación automática se produce antes de que caduque el certificado de firma de STS y antes de activar la alarma de caducidad de 90 días. Si se produce un error en la renovación automática, vCenter Single Sign-On crea un mensaje de error en el archivo de registro. Si es necesario, puede actualizar el certificado de firma de STS manualmente.

Nota vCenter Single Sign-On no realiza la renovación automática de certificados de firma de STS generados de forma personalizada o de terceros.

Actualizar y reemplazar certificados STS

En vSphere 8.0 y otras versiones posteriores, la actualización o la importación y el reemplazo de los certificados de firma de STS no requieren que se reinicie vCenter Server y, por lo tanto, evitan el tiempo de inactividad. Además, en una configuración vinculada, al actualizar o importar y reemplazar los certificados de firma de STS en un solo vCenter Server, se actualizan los certificados de STS en todos los sistemas vCenter Server vinculados.

Nota Una actualización o importación de certificados de firma de STS puede requerir que se reinicien manualmente los sistemas vCenter Server.

Actualizar un certificado vCenter Server STS mediante el vSphere Client

Puede actualizar los certificados de firma de STS vCenter Server mediante el vSphere Client. El VMware Certificate Authority (VMCA) emite un nuevo certificado y reemplaza el certificado actual.

Al actualizar los certificados de firma de STS, el VMware Certificate Authority (VMCA) emite un nuevo certificado y reemplaza el certificado actual en VMware Directory Service (vmdir). STS comienza a utilizar el nuevo certificado para emitir nuevos tokens. En una configuración de Enhanced Linked Mode, vmdir carga el nuevo certificado del sistema vCenter Server emisor a todos los sistemas vCenter Server vinculados. Al actualizar los certificados de firma de STS, debe reiniciar el sistema vCenter Server y cualquier otro sistema vCenter Server que forme parte de una configuración de Enhanced Linked Mode.

Si utiliza un certificado de firma de STS de terceros o generado personalizado, la actualización sobrescribe ese certificado con un certificado emitido por VMCA. Para actualizar certificados de firma de STS de terceros o generados de forma personalizada, utilice la opción importar y reemplazar. Consulte Importar y reemplazar un certificado vCenter Server STS mediante el vSphere Client.

El certificado de firma de STS emitido por VMCA es válido durante diez años y no es un certificado externo. No reemplace este certificado a menos que la directiva de seguridad de su empresa lo requiera.

Requisitos previos

Para la administración de certificados, debe proporcionar la contraseña del administrador del dominio local (administrator@vsphere.local de forma predeterminada). Si está renovando certificados, también puede proporcionar las credenciales de vCenter Single Sign-On para un usuario con privilegios de administrador en el sistema vCenter Server.

Procedimiento

1. Inicie sesión con vSphere Client en vCenter Server.
2. Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.
3. Desplácese hasta la interfaz de usuario de administración de certificados.
   a. En el menú **Inicio**, seleccione **Administración**.
   b. En **Certificados**, haga clic en **Administración de certificados**.
4. Si el sistema lo solicita, introduzca las credenciales de su instancia de vCenter Server.

5 En la pestaña **Firma de STS**, seleccione el certificado que desee y haga clic en **Actualizar con certificado de vCenter**.

   Si utiliza un certificado de firma de STS de terceros o generado personalizado, la acción de actualización sobrescribe ese certificado con un certificado generado por VMCA.

   Nota Si utilizaba certificados de terceros por motivos de cumplimiento, es posible que la actualización haga que los sistemas vCenter Server no cumplan con las directivas de conformidad. Además, si utiliza un certificado de firma de STS de terceros o generado personalizado, el servicio de token de seguridad ya no utiliza ese certificado personalizado o de terceros para la firma de tokens.

6 Haga clic en **Actualizar**.

   VMCA actualiza el certificado de firma de STS en este sistema vCenter Server y en cualquier sistema vCenter Server vinculado.

7 (opcional) Si aparece el botón **Forzar actualización**, vCenter Single Sign-On detectó un problema. Antes de hacer clic en **Forzar actualización**, tenga en cuenta los siguientes resultados potenciales.

   - Si todos los sistemas vCenter Server afectados no ejecutan al menos vSphere 7.0 Update 3, no admiten la actualización del certificado.
   - Si selecciona **Forzar actualización** requiere que reinicie todos los sistemas vCenter Server y que dichos sistemas no puedan funcionar hasta que usted lo haga.

   a Si no está seguro del impacto, haga clic en **Cancel** e investigue su entorno.

   b Si está seguro del impacto, haga clic en **Forzar actualización** para continuar con la actualización y, a continuación, reinicie manualmente los sistemas vCenter Server.

Importar y reemplazar un certificado vCenter Server STS mediante el vSphere Client

Puede importar y reemplazar el certificado vCenter Server STS por un certificado generado de forma personalizada o de terceros mediante el vSphere Client.

Para importar y reemplazar el certificado de firma de STS predeterminado, primero debe generar un nuevo certificado. Al importar y reemplazar certificados de firma de STS, el VMware Directory Service (vmdir) carga el nuevo certificado del sistema vCenter Server emisor en todos los sistemas vCenter Server vinculados.

El certificado STS no es un certificado externo. No reemplace este certificado a menos que la directiva de seguridad de su empresa lo requiera.

Requisitos previos

Para la administración de certificados, debe proporcionar la contraseña del administrador del dominio local (administrator@vsphere.local de forma predeterminada). También debe proporcionar las credenciales de vCenter Single Sign-On para un usuario con privilegios de administrador en el sistema vCenter Server.

Procedimiento

1. Inicie sesión con vSphere Client en vCenter Server.
2. Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.
3. Desplácese hasta la interfaz de usuario de administración de certificados.
   a. En el menú **Inicio**, seleccione **Administración**.
   b. En **Certificados**, haga clic en **Administración de certificados**.
4. Si el sistema lo solicita, introduzca las credenciales de su instancia de vCenter Server.
5. En la pestaña **Firma de STS**, seleccione el certificado que desee y haga clic en **Importar y reemplazar certificado**.
6. Seleccione el archivo PEM.

   El archivo PEM incluye la cadena de certificados de firma y la clave privada.
7. Haga clic en **Reemplazar**.

   El certificado de firma de STS se reemplaza en este sistema vCenter Server y en cualquier sistema de vCenter Server vinculado. A menos que se indique lo contrario, no es necesario reiniciar los sistemas vCenter Server.

Reemplazar un certificado vCenter Server STS mediante la línea de comandos

Puede reemplazar el certificado vCenter Server STS por un certificado de terceros o generado de forma personalizada mediante la CLI.

Para utilizar un certificado obligatorio de la empresa o para actualizar un certificado que está a punto de caducar, puede reemplazar el certificado de firma de STS existente. Para importar el certificado de firma de STS predeterminado, primero debe generar un nuevo certificado.

El certificado STS no es un certificado externo. No reemplace este certificado a menos que la directiva de seguridad de su empresa lo requiera.

Precaución Debe seguir los procedimientos que se describen a continuación. No reemplace el certificado directamente en el sistema de archivos.

Requisitos previos

Habilitar inicio de sesión en SSH en vCenter Server. Consulte Administrar vCenter Server mediante el shell de vCenter Server.

Procedimiento

1. Inicie sesión en el shell de vCenter Server como raíz.

2 Cree un certificado.

a Cree un directorio de nivel superior para mantener el nuevo certificado y compruebe la ubicación del directorio.

```
mkdir newsts
cd newsts
pwd
#resulting output: /root/newsts
```

b Copie el archivo `certool.cfg` en el nuevo directorio.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /root/newsts
```

c Utilizando un editor de línea de comandos, como Vim, abra una copia del archivo `certool.cfg` y edítela para usar el nombre de host y la dirección IP de vCenter Server local. El país es obligatorio y tiene que ser de dos caracteres, como se muestra en el siguiente ejemplo.

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

d Genere la clave.

```
/usr/lib/vmware-vmca/bin/certool --server localhost --genkey --privkey=/root/newsts/
sts.key --pubkey=/root/newsts/sts.pub
```

e Genere el certificado.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=/root/newsts/newsts.cer --privkey=/
root/newsts/sts.key --config=/root/newsts/certool.cfg
```

f Cree un archivo PEM con la cadena de certificados y la clave privada.

```
cat newsts.cer /var/lib/vmware/vmca/root.cer sts.key > newsts.pem
```

3 Actualice el certificado de firma de STS, por ejemplo:

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vsphere.local /root/newsts/newsts.pem
```

VMCA actualiza el certificado de firma de STS en este sistema vCenter Server y en cualquier sistema vCenter Server vinculado.

Ver la cadena de certificados de firma de STS vCenter Server activos mediante el vSphere Client

Puede utilizar vSphere Client para ver la cadena de certificados de firma de STS de la instancia de vCenter Server activa y la información de certificación, como la fecha de validez.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Introduzca el nombre de usuario y la contraseña de un usuario que tenga al menos privilegios de lectura.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Si el sistema lo solicita, introduzca las credenciales de su instancia de vCenter Server.

5 En la pestaña **Firma de STS**, seleccione un certificado y, a continuación, expanda el certificado.

   Se muestra información sobre el certificado y el problema, como:

   - Fecha de validez
   - Una marca de comprobación verde para un certificado válido y una marca de comprobación naranja de advertencia de un certificado caducado

Determinar la fecha de caducidad de un certificado SSL de LDAPS mediante la línea de comandos

Cuando se utiliza Active Directory en LDAP, puede cargar un certificado SSL para el tráfico LDAP. Los certificados SSL caducan después de un tiempo predefinido. Puede utilizar el comando `sso-config.sh` para ver la fecha de caducidad del certificado para que sepa cuándo reemplazar o renovar el certificado antes de que caduque.

vCenter Server le avisa cuando un certificado SSL de LDAP activo está próximo a su fecha de caducidad.

Solo puede ver la información de caducidad del certificado si utiliza un origen de identidad de OpenLDAP o Active Directory en LDAP, y si especifica una dirección URL `ldaps://` para el servidor.

Requisitos previos

Habilitar inicio de sesión en SSH en vCenter Server. Consulte Administrar vCenter Server mediante el shell de vCenter Server.

Procedimiento

1 Inicie sesión como raíz en vCenter Server.

2 Ejecute el siguiente comando.

```
/opt/vmware/bin/sso-config.sh -get_identity_sources
```

Ignore los mensajes de SLF4J.

3 Para determinar la fecha de caducidad, consulte los detalles del certificado SSL y compruebe el campo `NotAfter`.

Administrar directivas de vCenter Single Sign-On

Las directivas de vCenter Single Sign-On aplican las reglas de seguridad para las cuentas y los tokens locales en general. Puede ver y editar la directiva de contraseñas, la directiva de bloqueo y la directiva de tokens de vCenter Single Sign-On predeterminadas.

Editar la directiva de contraseñas de vCenter Single Sign-On

La directiva de contraseñas de vCenter Single Sign-On determina el formato y la caducidad de la contraseña. La directiva de contraseñas se aplica solo a los usuarios del dominio de vCenter Single Sign-On (vsphere.local).

De forma predeterminada, las contraseñas de cuenta de usuario integradas de vCenter Single Sign-On caducan a los 90 días. vSphere Client recuerda al usuario cuando la contraseña está a punto de caducar.

Consulte Cambiar la contraseña de vCenter Single Sign-On .

Nota La cuenta de administrador (administrator@vsphere.local) no se bloquea y la contraseña no caduca. Una práctica de seguridad adecuada es auditar los inicios de sesión desde esta cuenta y rotar la contraseña con regularidad.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

a En el menú **Inicio**, seleccione **Administración**.

b En **Single Sign On**, haga clic en **Configuración**.

4 Haga clic en la pestaña **Cuentas locales**.

5 Haga clic en **Editar** en la fila **Directiva de contraseña**.

6 Edite la directiva de contraseñas.

Opción	Descripción
Descripción	Descripción de directivas de contraseñas.
Duración máxima	Cantidad máxima de días de validez de la contraseña antes de que el usuario deba cambiarla. El número máximo de días que puede introducir es 999999999. Un valor de cero (0) significa que la contraseña nunca caduca.
Reutilización restringida	Cantidad de contraseñas anteriores que no pueden volver a utilizarse. Por ejemplo, si introduce 6, el usuario no puede volver a usar ninguna de las últimas seis contraseñas.
Longitud máxima	Cantidad máxima de caracteres que se permiten en la contraseña.
Longitud mínima	Cantidad mínima de caracteres que se requiere en la contraseña. La longitud mínima no debe ser inferior a la cantidad mínima requerida de caracteres alfabéticos, numéricos y especiales combinados.
Requisitos de caracteres	Cantidad mínima de tipos de caracteres diferentes que se requieren en la contraseña. Puede especificar la cantidad de caracteres de cada tipo de la siguiente manera: ■ Especiales: & # % ■ Alfabéticos: A b c D ■ Mayúsculas: A B C ■ Minúsculas: a b c ■ Numéricos: 1 2 3 ■ Adyacente idéntico: el número debe ser superior a 0. Por ejemplo, si escribe 1, la siguiente contraseña no se permite: p@$$word. La cantidad mínima de caracteres alfabéticos no debe ser inferior a la cantidad de caracteres en mayúscula y minúscula combinados. Se admiten caracteres no ASCII en las contraseñas. En versiones anteriores de vCenter Single Sign-On, hay limitaciones en los caracteres admitidos.

Nota La directiva de contraseñas selecciona el valor de longitud máxima solo si la longitud mínima es superior a 20 caracteres. El comportamiento de la directiva de contraseñas no está definido o podría provocar errores en los servicios cuando el valor de longitud mínima es superior a 20 caracteres y la longitud máxima está establecida en cualquier valor. Para evitar un posible problema, establezca la longitud mínima en el valor predeterminado de 8 caracteres, o no más de 20 caracteres.

7 Haga clic en **Guardar**.

Editar la directiva de bloqueo de vCenter Single Sign-On

Si un usuario intenta iniciar sesión con las credenciales equivocadas, una directiva de bloqueo de vCenter Single Sign-On especifica cuándo queda bloqueada la cuenta del usuario de vCenter Single Sign-On. Los administradores pueden editar la directiva de bloqueo.

Si un usuario inicia sesión varias veces en vsphere.local con la contraseña incorrecta, su cuenta se bloqueará. La directiva de bloqueo permite que los administradores especifiquen la cantidad máxima de intentos fallidos de inicio de sesión, y establezcan el intervalo entre un intento fallido y otro. En la directiva también se especifica cuánto tiempo debe transcurrir antes de que la cuenta se desbloquee automáticamente.

Nota La directiva de bloqueo se aplica únicamente a las cuentas de usuario, no a las cuentas de sistema, como administrator@vsphere.local.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 Haga clic en la pestaña **Cuentas locales**.

5 Haga clic en **Editar** en la fila **Directiva de bloqueo**.

   Es posible que deba desplazarse hacia abajo para ver la fila **Directiva de bloqueo**.

6 Edite los parámetros.

Opción	Descripción
Descripción	Descripción opcional de la directiva de bloqueo.
Cantidad máxima de intentos fallidos de inicio de sesión	Cantidad máxima de intentos fallidos de inicio de sesión permitidos antes de que la cuenta se bloquee.
Intervalo entre intentos fallidos	Período en el cual deben ocurrir los intentos fallidos de inicio de sesión para activar un bloqueo.
Tiempo de desbloqueo	Cantidad de tiempo durante la cual permanece bloqueada la cuenta. Si introduce 0, el administrador debe desbloquear la cuenta explícitamente.

7 Haga clic en **Guardar**.

Editar la directiva de tokens de vCenter Single Sign-On

La directiva de tokens de vCenter Single Sign-On especifica las propiedades de tokens, como la tolerancia de reloj y el recuento de renovaciones. Puede editar la directiva de tokens para que la especificación de los tokens se adapte a los estándares de seguridad de la empresa.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 Haga clic en la pestaña **Cuentas locales**.

5 Haga clic en **Editar** en la fila **Confiabilidad de tokens**.

   Es posible que deba desplazarse hacia abajo para ver la fila **Confiabilidad de tokens**.

6 Edite los parámetros de configuración de la directiva de tokens.

Opción	Descripción
Tolerancia de reloj	Diferencia horaria, en milisegundos, que vCenter Single Sign-On tolera entre un reloj de cliente y el reloj de la controladora de dominio. Si la diferencia horaria es mayor que el valor especificado, vCenter Single Sign-On declara al token como no válido.
Recuento máximo de renovaciones de token	Es la máxima cantidad de veces que puede renovarse un token. Una vez alcanzada la cantidad máxima de intentos de renovación, se requiere un nuevo token de seguridad.
Recuento máximo de delegaciones de token	Los tokens HoK (Holder-of-key) pueden delegarse a servicios del entorno vSphere. Un servicio que emplea un token delegado ejecuta dicho servicio en nombre del servicio principal que proporcionó el token. La solicitud de un token especifica una identidad DelegateTo. El valor de DelegateTo puede ser el token de una solución o una referencia al token de la solución. Este valor especifica cuántas veces puede delegarse un mismo token HoK.
Duración máxima de token de portador	Los tokens de portador proporcionan autenticación basada únicamente en la posesión del token. Los tokens de portador están pensados para el uso a corto plazo y para una única operación. El token de portador no comprueba la identidad del usuario o de la entidad que envía la solicitud. Este valor especifica la duración del token de portador antes de que el token deba emitirse nuevamente.
Duración máxima de token HoK	Los tokens HoK proporcionan autenticación basada en los artefactos de seguridad que están integrados en el token. Los tokens HoK pueden usarse para operaciones de delegación. Un cliente puede obtener un token HoK y delegarlo a otra entidad. El token contiene las notificaciones para identificar al originador y al delegado. En el entorno vSphere, un sistema vCenter Server obtiene tokens delegados en nombre de un usuario y los utiliza para realizar operaciones. Este valor determina la duración de un token HoK antes de que el token se marque como no válido.

7 Haga clic en **Guardar**.

Editar la notificación de caducidad de contraseña para usuarios de Active Directory (autenticación integrada de Windows)

La notificación de caducidad de la contraseña de Active Directory se realiza de manera independiente de la caducidad de la contraseña de vCenter Server SSO. De forma predeterminada, la notificación de caducidad de la contraseña para un usuario de Active Directory se envía tras 30 días, pero la fecha de caducidad real de la contraseña depende del sistema de Active Directory. vSphere Client controla la notificación de caducidad. Puede cambiar la notificación de caducidad predeterminada para cumplir con los estándares de seguridad de su empresa.

Requisitos previos

- Habilitar inicio de sesión en SSH en vCenter Server. Consulte Administrar vCenter Server mediante el shell de vCenter Server.

Procedimiento

1 Inicie sesión en el shell de vCenter Server como usuario con privilegios de administrador.

  El usuario predeterminado con la función de superadministrador es root.

2 Cambie el directorio a la ubicación del archivo vSphere Client `webclient.properties`.

```
cd /etc/vmware/vsphere-ui
```

3 Abra el archivo `webclient.properties` con un editor de texto.

4 Edite la siguiente variable.

```
sso.pending.password.expiration.notification.days = 30
```

5 Reinicie el vSphere Client.

```
service-control --stop vsphere-ui
service-control --start vsphere-ui
```

Administrar usuarios y grupos de vCenter Single Sign-On

Un usuario administrador de vCenter Single Sign-On puede administrar usuarios y grupos en el dominio vsphere.local desde vSphere Client.

vSphere Client presenta una vista de usuarios y grupos en el dominio de vSphere (vsphere.local de forma predeterminada). Desde esta vista, puede agregar, editar y desactivar usuarios. También puede agregar grupos y administrar la pertenencia a grupos.

Agregar usuarios de vCenter Single Sign-On

Los usuarios que aparecen en la pestaña **Usuarios** en vSphere Client son internos de vCenter Single Sign-On y pertenecen al dominio vsphere.local. Puede agregar usuarios a ese dominio en una de las interfaces de administración de vCenter Single Sign-On.

Puede seleccionar otros dominios y ver en ellos información sobre los usuarios, pero no puede agregar usuarios a otros dominios desde una interfaz de administración de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Si el dominio actualmente seleccionado no es vsphere.local, selecciónelo en el menú desplegable.

   No puede agregar usuarios a otros dominios.

5 En la pestaña **Usuarios**, haga clic en **Agregar**.

6 Escriba un nombre de usuario y una contraseña para el nuevo usuario.

   El número máximo de caracteres permitido para el nombre de usuario es 300.

   No puede cambiar el nombre de usuario una vez creado el usuario. La contraseña debe cumplir con los requisitos de la directiva de contraseñas del sistema.

7 (opcional) Introduzca el nombre y los apellidos del nuevo usuario.

8 (opcional) Introduzca una dirección de correo electrónico y una descripción del usuario.

9 Haga clic en **Agregar**.

Resultados

Cuando agrega un usuario, este en principio no tiene privilegios para realizar operaciones de administración.

Pasos siguientes

Agregue el usuario a un grupo del dominio vsphere.local, por ejemplo, al grupo de usuarios que pueden administrar VMCA (Administradores de CA) o al grupo de usuarios que pueden administrar vCenter Single Sign-On (Administradores). Consulte Agregar miembros a un grupo de vCenter Single Sign-On.

Desactivar y activar usuarios de vCenter Single Sign-On

Cuando se desactiva una cuenta de usuario de vCenter Single Sign-On, el usuario no puede iniciar sesión en el servidor de vCenter Single Sign-On hasta que un administrador active la cuenta. Es posible desactivar y activar cuentas desde una de las interfaces de administración de vCenter Single Sign-On.

Las cuentas de usuario desactivadas permanecen disponibles en el sistema vCenter Single Sign-On, pero el usuario no puede iniciar sesión ni realizar operaciones en el servidor. Los usuarios con privilegios de administrador pueden desactivar y activar cuentas desde la página **Usuarios y grupos** de vCenter Server.

Requisitos previos

Debe ser miembro del grupo de administradores de vCenter Single Sign-On para desactivar y activar usuarios de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Seleccione un nombre de usuario y haga clic en **Más**; a continuación, haga clic en **Deshabilitar**.

5 Haga clic en **Aceptar**.

6 Para volver a activar el usuario, haga clic en **Más**, haga clic en **Habilitar** y, a continuación, en **Aceptar**.

Eliminar un usuario de vCenter Single Sign-On

Puede eliminar usuarios que se encuentran en el dominio vsphere.local desde una interfaz de administración de vCenter Single Sign-On. No puede eliminar usuarios del sistema operativo local ni usuarios de otro dominio desde una interfaz de administración de vCenter Single Sign-On.

Precaución Si elimina el usuario administrador del dominio vsphere.local, ya no podrá iniciar sesión en vCenter Single Sign-On. Reinstale vCenter Server y sus componentes.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Seleccione **Usuarios** y el dominio vsphere.local en el menú desplegable.

5 En la lista de usuarios seleccione el usuario que desea eliminar.

6 Haga clic en **Eliminar**.

   Proceda con precaución, ya que esta acción no se puede deshacer.

7 Haga clic en **Quitar**.

Editar un usuario de vCenter Single Sign-On

Puede cambiar la contraseña u otros detalles de un usuario de vCenter Single Sign-On desde una interfaz de administración de vCenter Single Sign-On. No puede cambiar el nombre de los usuarios en el dominio vsphere.local. Esto significa que no puede cambiar el nombre de administrator@vsphere.local.

Puede crear usuarios adicionales con los mismos privilegios de administrator@vsphere.local.

Los usuarios de vCenter Single Sign-On se almacenan en el dominio vsphere.local de vCenter Single Sign-On.

Puede revisar las directivas sobre contraseñas de vCenter Single Sign-On desde vSphere Client. Inicie sesión como administrator@vsphere.local y en el menú **Administración**, seleccione **Configuración > Cuentas locales > Directiva de contraseñas**.

Consulte también Editar la directiva de contraseñas de vCenter Single Sign-On.

Procedimiento

1. Inicie sesión con vSphere Client en vCenter Server.
2. Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.
3. Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.
   a. En el menú **Inicio**, seleccione **Administración**.
   b. En **Single Sign-On**, haga clic en **Usuarios y grupos**.
4. Haga clic en **Usuarios**.
5. Seleccione el usuario y haga clic en **Editar**.
6. Edite los atributos del usuario.

   No puede cambiar el nombre de usuario.

   La contraseña debe cumplir con los requisitos de la directiva de contraseñas del sistema.
7. Haga clic en **Guardar**.

Agregar un grupo de vCenter Single Sign-On

La pestaña **Grupos** de vCenter Single Sign-On muestra los grupos del dominio local (de manera predeterminada, vsphere.local). Puede agregar grupos si necesita un contenedor para miembros de grupos (entidades de seguridad).

No puede agregar grupos a otros dominios (por ejemplo, el dominio de Active Directory) desde la pestaña **Grupos** de vCenter Single Sign-On.

Si no agrega un origen de identidad a vCenter Single Sign-On, la creación de grupos y la incorporación de usuarios pueden ayudarlo a organizar el dominio local.

Procedimiento

1. Inicie sesión con vSphere Client en vCenter Server.
2. Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.
3. Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.
   a. En el menú **Inicio**, seleccione **Administración**.
   b. En **Single Sign-On**, haga clic en **Usuarios y grupos**.
4. Seleccione **Grupos** y haga clic en **Crear grupo**.

5 Introduzca un nombre y una descripción para el grupo.

   El número máximo de caracteres permitido para el nombre de grupo es 300. No puede cambiar el nombre de grupo una vez creado el grupo.

6 En el menú desplegable **Agregar miembros**, seleccione el origen de identidad que contiene el miembro que se agregará al grupo.

   Si configuró un proveedor de identidad externo, como AD FS, el dominio de dicho proveedor de identidad estará disponible para seleccionarlo en el menú desplegable **Agregar miembros**.

7 Introduzca un término de búsqueda.

8 Seleccione al miembro.

   Puede agregar más de un miembro.

9 Haga clic en **Listo**.

Pasos siguientes

Consulte Agregar miembros a un grupo de vCenter Single Sign-On.

Agregar miembros a un grupo de vCenter Single Sign-On

Los miembros de un grupo de vCenter Single Sign-On pueden ser usuarios u otros grupos de uno o más orígenes de identidad. Puede agregar miembros nuevos de vSphere Client.

Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2095342 para obtener información del contexto.

Los grupos que se enumeran en la pestaña **Grupos** de la interfaz web son parte del dominio vsphere.local. Consulte Grupos del dominio de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Haga clic en la pestaña **Grupos** y, a continuación, en el grupo (por ejemplo, Administradores).

5 Haga clic en **Editar**.

6 En el menú desplegable **Dominio**, seleccione el origen de identidad que contiene el miembro que se agregará al grupo.

   Si configuró un proveedor de identidad externo, como AD FS, el dominio de ese proveedor de identidad estará disponible para seleccionarlo en el menú desplegable **Dominio**.

7 Introduzca un término de búsqueda.

8 Seleccione al miembro.

   Puede agregar más de un miembro.

9 Para entornos de vSphere+, si selecciona **VMware ID** en el menú desplegable **Dominio**, a continuación tendrá que introducir el nombre de la cuenta de CSP en el campo **Nombre de usuario**.

   Nota Introduzca la dirección de correo electrónico de la cuenta de CSP en el campo **Nombre de usuario**. No se pueden buscar cuentas de CSP en el dominio VMwareID.

   ---

10 Haga clic en **Guardar**.

Quitar miembros de un grupo de vCenter Single Sign-On

Es posible eliminar miembros de un grupo de vCenter Single Sign-On mediante vSphere Client. Al quitar un miembro (usuario o grupo) de un grupo local, el miembro no se elimina del sistema.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Haga clic en **Grupos** y seleccione un grupo.

5 Haga clic en **Editar**.

6 En la lista Miembros actuales, haga clic en el usuario o grupo que desea eliminar.

7 Haga clic en **Listo**.

Resultados

El usuario o grupo se elimina del grupo, pero sigue disponible en el sistema.

Cambiar la contraseña de vCenter Single Sign-On

Los usuarios del dominio local, vsphere.local de forma predeterminada, pueden cambiar sus contraseñas de vCenter Single Sign-On desde vSphere Client. Los usuarios de otros dominios pueden cambiar la contraseña mediante las reglas de ese dominio.

La directiva de bloqueo de vCenter Single Sign-On determina el momento en que caduca la contraseña. De forma predeterminada, las contraseñas de vCenter Single Sign-On caducan a los 90 días, pero las contraseñas de administrador, como la de administrator@vsphere.local, no caducan. Las interfaces de administración de vCenter Single Sign-On muestran una advertencia cuando la contraseña está por caducar.

Nota Solo puede cambiar una contraseña si no ha caducado.

Si la contraseña ha caducado, el administrador del dominio local, administrator@vsphere.local de forma predeterminada, puede restablecerla mediante el comando `dir-cli password reset`. Solo pueden restablecer contraseñas los miembros del grupo Administrador para el dominio de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 En el panel de navegación superior, haga clic en el nombre de usuario para acceder al menú y seleccione **Cambiar contraseña**.

4 Introduzca la contraseña actual.

5 Introduzca una contraseña nueva y confírmela.

   La contraseña debe cumplir con la directiva de contraseñas.

6 Haga clic en **Confirmar**.

   Como alternativa, puede seleccionar **Single Sign On > Usuarios y grupos**, seleccionar el usuario y hacer clic en **Editar**.

Opciones de autenticación de vSphere

En vSphere 7.0 y versiones posteriores, la federación de proveedores de identidad externos es el método de autenticación preferido en vCenter Server. Todavía puede autenticarse a través de una tarjeta inteligente (tarjeta de acceso común —Common Access Card, CAC— basada en UPN) o mediante un token RSA SecurID.

Métodos de autenticación de dos factores

Las agencias gubernamentales o las grandes empresas a menudo requieren la autenticación de dos factores. vSphere admite los siguientes métodos de autenticación en dos fases .

Federación de proveedores de identidad externos

Con la federación de proveedores de identidad externos, puede utilizar los mecanismos de autenticación compatibles con el proveedor de identidad externo, incluida la autenticación multifactor.

Autenticación de tarjeta inteligente

La autenticación de tarjeta inteligente solo permite el acceso a usuarios que conectan un lector de tarjeta física al equipo donde inician sesión. Un ejemplo es la autenticación de tarjeta de acceso común (Common Access Card, CAC).

El administrador puede implementar la PKI para que los certificados de tarjeta inteligente sean los únicos certificados de cliente que emita la CA. En estas implementaciones, al usuario solo se le presentan certificados de tarjeta inteligente. El usuario selecciona un certificado y se le solicita un PIN. Solo los usuarios que tienen tarjeta física y el PIN que coincide con el certificado pueden iniciar sesión.

Autenticación de RSA SecurID

Para utilizar la autenticación de RSA SecurID, el entorno debe incluir una instancia de RSA Authentication Manager configurada correctamente. Si vCenter Server está configurado para apuntar al servidor RSA, y si la autenticación de RSA SecurID está activada, los usuarios pueden iniciar sesión con su nombre de usuario y su token.

Para obtener más información, consulte la publicación del blog de vSphere, Configuración de RSA SecurID.

Nota vCenter Single Sign-On solo admite SecurID nativo. No admite la autenticación RADIUS .

Especificar un vCenter Server método de autenticación no predeterminado

Es posible configurar un método de autenticación no predeterminado en vSphere Client o mediante el script `sso-config`.

- Para la autenticación de tarjeta inteligente, puede realizar la configuración de vCenter Single Sign-On desde vSphere Client o mediante `sso-config`. La configuración incluye la activación de la autenticación de tarjetas inteligentes y la configuración de las políticas de revocación de certificados.

- En el caso de RSA SecurID, puede utilizar el script `sso-config` para configurar RSA Authentication Manager para el dominio y para habilitar la autenticación de token de RSA. La autenticación de RSA SecurID no puede configurarse desde vSphere Client. Sin embargo, si habilita RSA SecurID, ese método de autenticación aparece en vSphere Client.

Combinar métodos de autenticación vCenter Server

Los métodos de autenticación se pueden activar o desactivar de forma separada utilizando `sso-config`. Inicialmente, deje habilitada la autenticación por nombre de usuario y contraseña mientras prueba un método de autenticación de dos factores; después de las pruebas, habilite un único método de autenticación.

Inicio de sesión de autenticación de tarjeta inteligente

Una tarjeta inteligente es una tarjeta plástica pequeña con un chip de circuito integrado. Muchas agencias gubernamentales y empresas grandes utilizan tarjetas inteligentes como tarjetas de acceso común (CAC) para incrementar la seguridad de los sistemas y cumplir con las normas de seguridad. Se utiliza una tarjeta inteligente en aquellos entornos donde todas las máquinas incluyen un lector para este tipo de tarjetas. Los controladores del hardware de tarjetas inteligentes que las gestionan suelen estar preinstalados.

Nota En vSphere 7.0 Update 2 y versiones posteriores, puede habilitar FIPS en vCenter Server. Consulte la documentación de *Seguridad de vSphere*. Las autenticaciones RSA SecureID y CAC no se admiten cuando FIPS está habilitado. Utilice la federación de proveedores de identidad externos para la autenticación MFA. Consulte Configurar la federación de proveedores de identidad de vCenter Server.

A los usuarios que inician sesión en un sistema vCenter Server se les pide que realicen la autenticación con una combinación de tarjeta inteligente y PIN, como se indica a continuación.

1 Cuando se introduce una tarjeta inteligente en el lector de tarjetas inteligentes, el explorador lee los certificados en la tarjeta.

2 El explorador solicita al usuario que seleccione un certificado y luego le solicita el PIN correspondiente a dicho certificado.

3 vCenter Single Sign-On comprueba si se conoce el certificado de la tarjeta inteligente. Si la verificación de revocación está activa, vCenter Single Sign-On también verifica si el certificado fue revocado.

4 Si vCenter Single Sign-On conoce el certificado, y este no es un certificado revocado, el usuario es autenticado y puede realizar las tareas para las que tiene permisos.

Nota Generalmente, es lógico dejar la autenticación por nombre y contraseña activada durante las pruebas. Una vez completada la prueba, deshabilite la autenticación por nombre de usuario y contraseña, y habilite la autenticación de tarjeta inteligente. Después, vSphere Client solo admitirá el inicio de sesión de tarjeta inteligente. Solo los usuarios con privilegios de raíz o administrador en la máquina podrán reactivar la autenticación por nombre de usuario y contraseña iniciando sesión directamente en vCenter Server.

Configurar y usar la autenticación de tarjeta inteligente

El entorno puede configurarse para que requiera autenticación de tarjeta inteligente cuando un usuario se conecta a vCenter Server desde vSphere Client.

La configuración de la autenticación con tarjeta inteligente implica los siguientes pasos detallados:

1 Configurar el sistema vCenter Server para solicitar certificados de cliente.

2 Activando la configuración de la tarjeta inteligente.

   Puede utilizar la utilidad vSphere Client o `sso-config` para activar la configuración.

3 Personalizar la comprobación de revocación de certificados.

   Puede usar la utilidad vSphere Client o `sso-config` para personalizar la comprobación.

Configurar vCenter Server para solicitar certificados de cliente

Antes de activar la autenticación con tarjeta inteligente, debe configurar vCenter Server para solicitar certificados de cliente.

La configuración utiliza el puerto 3128 que se establece y se abre automáticamente en vCenter Server.

Requisitos previos

Copie los certificados de la entidad de certificación (CA) en el sistema vCenter Server a fin de usarlos para crear el almacén de CA cliente de confianza. Este almacén debe contener los certificados de confianza emitidos por la CA para el certificado de cliente. El cliente aquí es el explorador desde el que el proceso de la tarjeta inteligente solicita información al usuario final.

Nota vCenter Server 7.0 y las versiones posteriores son compatibles con el protocolo HTTP/2. Todos los navegadores y las aplicaciones modernas, incluido vSphere Client, se conectan a vCenter Server mediante HTTP/2. Sin embargo, la autenticación de tarjeta inteligente requiere el uso del protocolo HTTP/1.1. Al activar la autenticación de tarjeta inteligente, se desactiva la negociación del protocolo de la capa de aplicación (ALPN, del inglés "Application-Layer Protocol Negotiation", https://tools.ietf.org/html/rfc7301) para HTTP/2, lo que impide que el explorador utilice HTTP/2. Las aplicaciones que usen solo HTTP/2, sin depender de ALPN, seguirán funcionando.

Para completar la autenticación de tarjeta inteligente, se debe permitir que los clientes accedan al puerto 3128/TCP en la instancia de vCenter Server adecuada. Compruebe los firewalls perimetrales para asegurarse de que se le ha concedido acceso.

La conexión se redirecciona al puerto 3128 durante el inicio de sesión de la tarjeta inteligente. El puerto 3128 solo admite conexiones de autenticación mutua preconfiguradas y no está pensado como un endpoint de navegador directo. No devuelve un encabezado de HSTS. Si el escáner de vulnerabilidades informa de este comportamiento, se puede ignorar de forma segura.

Procedimiento

1 Inicie sesión en el shell de vCenter Server como usuario raíz.

2 Cree un almacén de CA de cliente de confianza en vCenter Server mediante la ruta de acceso exacta y el nombre PEM, `/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem`.

Advertencia Debe utilizar la ruta de acceso exacta y el nombre PEM, `/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem`.

a Cambie al directorio `/usr/lib/vmware-sso/`.

```
cd /usr/lib/vmware-sso/
```

b Para crear el almacén de CA de cliente de confianza, ejecute el comando `openssl` y tome como entrada el certificado de firma de confianza. Por ejemplo, el siguiente comando crea el archivo `clienttrustCA.pem` desde el certificado de firma de confianza `xyzCompanySmartCardSigningCA.cer`.

```
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/
vmware-sts/conf/clienttrustCA.pem
```

Puede agregar certificados adicionales al almacén de CA del cliente de confianza ejecutando el comando `openssl` con el operador ">>" para anexar el certificado adicional. Por ejemplo, el siguiente comando anexa `xyzCompanySmartCardSigningCA2.cer` al archivo `clienttrustCA.pem` existente.

```
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA2.cer >> /usr/lib/vmware-sso/
vmware-sts/conf/clienttrustCA.pem
```

3 Para validar que el contenido del archivo `clienttrustCA.pem` contenga las CA de confianza que firmaron los certificados de tarjeta inteligente, ejecute el comando `keytool`.

Por ejemplo:

```
keytool -printcert -file /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem | grep -i
"owner\|sha1\|issuer:\|valid"
```

4 Compruebe que los nombres de CA coincidan con la cadena de certificados de usuario de tarjeta inteligente.

Por ejemplo, puede ejecutar el siguiente comando.

```
sso-config.sh -get_authn_policy -t vsphere.local | grep trusted
```

Los certificados raíz e intermedios deben coincidir en huellas, nombres, fechas de validez, etc.

Nota También puede usar vSphere Client (**Administración > Single Sign On > Configuración > Proveedor de identidad > Autenticación de tarjeta inteligente > Configuración de la autenticación de tarjeta inteligente > Certificados de CA de confianza > Agregar**).

5 Reinicie el servicio STS.

```
service-control --restart sts
```

Administrar la autenticación de tarjeta inteligente mediante vSphere Client

Puede activar o desactivar la autenticación de tarjeta inteligente, personalizar el banner de inicio de sesión y configurar la directiva de revocación desde vSphere Client.

Si se activa la autenticación de tarjeta inteligente y se desactivan otros métodos de autenticación, se solicitará luego a los usuarios que inicien sesión con la autenticación de tarjeta inteligente.

Si se desactiva la autenticación con nombre de usuario y contraseña, y si hay problemas con la autenticación de tarjeta inteligente, los usuarios no podrán iniciar sesión. En ese caso, un usuario raíz o un usuario administrador pueden activar la autenticación con nombre de usuario y contraseña en la línea de comandos de vCenter Server. El siguiente comando activa la autenticación con nombre de usuario y contraseña.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

Requisitos previos

- Compruebe que en su entorno se haya configurado una infraestructura de clave pública (Public Key Infrastructure, PKI) empresarial, y que los certificados cumplan con los siguientes requerimientos:
  - Un nombre principal de usuario (User Principal Name, UPN) debe corresponder a una cuenta de Active Directory en la extensión del nombre alternativo del firmante (Subject Alternative Name, SAN).
  - El certificado debe especificar la autenticación del cliente en los campos Directiva de aplicación o Uso mejorado de clave; de lo contrario, el explorador no mostrará el certificado.
- Agregue un origen de identidad de Active Directory a vCenter Single Sign-On.

- Asigne la función de Administrador de vCenter Server a uno o más usuarios en el origen de identidad de Active Directory. Posteriormente, esos usuarios pueden realizar tareas de autenticación debido a que poseen privilegios de administrador de vCenter Server.
- Asegúrese de haber configurado el proxy inverso y reinicie el equipo físico o la máquina virtual.

Procedimiento

1. Obtenga los certificados y cópielos en una carpeta que la utilidad `sso-config` pueda ver.
   a. Inicie sesión en la consola de vCenter Server, ya sea directamente o a través de SSH.
   b. Active el shell de la siguiente manera.

   ```
   Command> shell
   chsh -s "/bin/bash" root
   chsh -s "bin/appliancesh" root
   ```

   c. Utilice WinSCP o una utilidad similar para copiar los certificados en el directorio `/usr/lib/vmware-sso/vmware-sts/conf` en la instancia de vCenter Server.
   d. Opcionalmente desactive el shell de la siguiente manera.

   ```
   chsh -s "/bin/appliancesh" root
   ```

2. Inicie sesión con vSphere Client en vCenter Server.
3. Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.
4. Desplácese hasta la interfaz de usuario de configuración.
   a. En el menú **Inicio**, seleccione **Administración**.
   b. En **Single Sign On**, haga clic en **Configuración**.
5. En la pestaña **Proveedor de identidad**, haga clic en **Autenticación de tarjeta inteligente** y, a continuación, haga clic en **Editar**.
6. Seleccione o anule la selección de los métodos de autenticación y haga clic en **Guardar**.

   No puede activar ni desactivar la autenticación RSA SecurID desde esta interfaz web. Sin embargo, si se activó RSA SecurID desde la línea de comandos, el estado aparece en la interfaz web.

   Aparece la pestaña **Certificados de CA de confianza**.
7. En la pestaña **Certificados de CA de confianza**:
   a. Haga clic en **Agregar** y en **Examinar**.
   b. Seleccione un certificado de CA de confianza y haga clic en **Agregar**.
8. Para agregar certificados de CA de confianza adicionales, repita el paso 7.

Pasos siguientes

El entorno puede requerir una configuración de OCSP mejorada.

- Si la respuesta OCSP es emitida por una CA distinta de la CA firmante de la tarjeta inteligente, proporcione el certificado de CA de firma correspondiente a OCSP.
- Puede configurar uno o más respondedores OCSP locales para cada sitio de vCenter Server en una implementación de varios sitios. Es posible configurar estos respondedores OCSP alternativos mediante la CLI. Consulte Administrar la autenticación de tarjeta inteligente mediante la CLI.

Administrar la autenticación de tarjeta inteligente mediante la CLI

La utilidad `sso-config` se puede utilizar para administrar la autenticación de tarjeta inteligente desde la línea de comandos. La utilidad admite todas las tareas de configuración de tarjeta inteligente.

Puede encontrar el script de `sso-config` en la siguiente ubicación:

```
/opt/vmware/bin/sso-config.sh
```

La configuración de los tipos de autenticación admitidos y la configuración de revocación se almacenan en VMware Directory Service y se replican en todas las instancias de vCenter Server en un dominio de vCenter Single Sign-On.

Si se desactiva la autenticación con nombre de usuario y contraseña, y si hay problemas con la autenticación de tarjeta inteligente, los usuarios no podrán iniciar sesión. En ese caso, un usuario raíz o un usuario administrador pueden activar la autenticación con nombre de usuario y contraseña en la línea de comandos de vCenter Server. El siguiente comando activa la autenticación con nombre de usuario y contraseña.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

Si utiliza el tenant predeterminado, use vsphere.local como nombre de tenant.

Si utiliza OCSP para la comprobación de revocación, puede basarse en el OCSP predeterminado que se especificó en la extensión AIA del certificado de tarjeta inteligente. También se puede anular la opción predeterminada y configurar uno o más respondedores OCSP alternativos. Por ejemplo, se pueden configurar respondedores OCSP locales en el sitio de vCenter Single Sign-On para procesar la solicitud de comprobación de revocación.

Nota Si el certificado no tiene un OCSP definido, habilite en cambio la CRL (lista de revocación de certificados).

Requisitos previos

- Compruebe que en su entorno se haya configurado una infraestructura de clave pública (Public Key Infrastructure, PKI) empresarial, y que los certificados cumplan con los siguientes requerimientos:
  - Un nombre principal de usuario (User Principal Name, UPN) debe corresponder a una cuenta de Active Directory en la extensión del nombre alternativo del firmante (Subject Alternative Name, SAN).
  - El certificado debe especificar la autenticación del cliente en los campos Directiva de aplicación o Uso mejorado de clave; de lo contrario, el explorador no mostrará el certificado.
- Agregue un origen de identidad de Active Directory a vCenter Single Sign-On.
- Asigne la función de Administrador de vCenter Server a uno o más usuarios en el origen de identidad de Active Directory. Posteriormente, esos usuarios pueden realizar tareas de autenticación debido a que poseen privilegios de administrador de vCenter Server.
- Asegúrese de haber configurado el proxy inverso y reinicie el equipo físico o la máquina virtual.

Procedimiento

1 Obtenga los certificados y cópielos en una carpeta que la utilidad `sso-config` pueda ver.

   a Inicie sesión en la consola de dispositivos, ya sea directamente o a través de SSH.

   b Active el shell del dispositivo de la siguiente manera.

   ```
   shell
   chsh -s "/bin/bash" root
   ```

   c Utilice WinSCP o una utilidad similar para copiar los certificados en `/usr/lib/vmware-sso/vmware-sts/conf` en la instancia de vCenter Server.

   d Opcionalmente desactive el shell de la siguiente manera.

   ```
   chsh -s "/bin/appliancesh" root
   ```

2 Para activar la autenticación de carrito inteligente, ejecute el siguiente comando.

   ```
   sso-config.sh -set_authn_policy -certAuthn true -cacerts
   first_trusted_cert.cer,second_trusted_cert.cer  -t tenant
   ```

   Por ejemplo:

   ```
   sso-config.sh -set_authn_policy -certAuthn true -cacerts MySmartCA1.cer,MySmartCA2.cer  -t
   vsphere.local
   ```

   Separe los distintos certificados con comas, pero no incluya espacios después de la coma.

3 Para desactivar todos los demás métodos de autenticación, ejecute los siguientes comandos.

```
sso-config.sh -set_authn_policy -pwdAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -winAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -securIDAuthn false -t vsphere.local
```

4 (opcional) Para establecer una lista de permitidos de directivas de certificado, ejecute el siguiente comando.

```
sso-config.sh -set_authn_policy -certPolicies policies
```

Para especificar varias directivas, sepárelas con una coma, por ejemplo:

```
sso-config.sh -set_authn_policy -certPolicies
2.16.840.1.101.2.1.11.9,2.16.840.1.101.2.1.11.19
```

La lista de permitidos especifica los identificadores de objeto de las directivas que están permitidas en la extensión de directiva de certificados del certificado. Los certificados X509 pueden tener una extensión de directiva de certificados.

5 (opcional) Active y configure la comprobación de revocación mediante OCSP.

a Active la comprobación de revocación mediante OCSP.

```
sso-config.sh  -set_authn_policy -t tenantName  -useOcsp true
```

b Si el vínculo del respondedor OCSP no se proporciona mediante la extensión AIA de los certificados, proporcione la URL del respondedor OCSP de anulación y el certificado de autoridad de OCSP.

El OCSP alternativo se configura para cada sitio de vCenter Single Sign-On. Es posible especificar más de un respondedor OCSP alternativo para el sitio de vCenter Single Sign-On de modo que permita la conmutación por error.

```
sso-config.sh -t tenant -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl http://
ocsp.xyz.com/ -ocspSigningCert yourOcspSigningCA.cer
```

Nota La configuración se aplica al sitio actual de vCenter Single Sign-On de forma predeterminada. Especifique el parámetro `siteID` únicamente si se configura un OCSP alternativo para otros sitios de vCenter Single Sign-On.

Tenga en cuenta el ejemplo siguiente:

```
 .sso-config.sh -t vsphere.local -add_alt_ocsp
-ocspUrl http://failover.ocsp.nsn0.rcvs.nit.disa.mil/ -ocspSigningCert ./
DOD_JITC_EMAIL_CA-29__0x01A5__DOD_JITC_ROOT_CA_2.cer
 Adding alternative OCSP responder for tenant :vsphere.local
 OCSP responder is added successfully!
 [
 site::   78564172-2508-4b3a-b903-23de29a2c342
     [
     OCSP url::   http://ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
     [
     OCSP url::   http://failover.ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
 ]
```

c Para mostrar la configuración del respondedor OCSP alternativo actual, ejecute este comando.

```
sso-config.sh -t tenantName -get_alt_ocsp]
```

d Para quitar la configuración del respondedor OCSP alternativo actual, ejecute este comando.

```
sso-config.sh -t tenantName -delete_alt_ocsp [-allSite] [-siteID
pscSiteID_for_the_configuration]
```

6 (opcional) Para hacer una lista de la información de configuración, ejecute el siguiente comando.

```
sso-config.sh -get_authn_policy -t tenantName
```

Configurar directivas de revocación para autenticación de tarjeta inteligente

Puede personalizar la verificación de revocación de certificados, así como especificar en qué lugar vCenter Single Sign-On busca información sobre certificados revocados.

Puede personalizar el comportamiento utilizando vSphere Client o el script de `sso-config`. La configuración seleccionada depende en parte de lo que la CA admite.

- Si la verificación de revocación está desactivada, vCenter Single Sign-On ignora cualquier configuración de CRL o OCSP. vCenter Single Sign-On no realiza comprobaciones sobre ningún certificado.
- Si la verificación de revocación está activada, la configuración depende de la configuración de la PKI.

  Solo OCSP

  Si la CA emisora admite un respondedor OCSP, active **OCSP** y desactive **CRL como conmutación por error para OCSP**.

  Solo CRL

  Si la CA emisora no admite OSCP, active la **verificación de CRL** y desactive la **verificación de OSCP**.

  Tanto OSCP como CRL

  Si la CA emisora admite tanto un respondedor OCSP como CRL, vCenter Single Sign-On verifica el respondedor OCSP primero. Si el respondedor devuelve un estado desconocido o no está disponible, vCenter Single Sign-On verifica la CRL primero. En este caso, active la **verificación de OCSP** y la **verificación de CRL**, y active **CRL como conmutación por error para OCSP**.
- Si la verificación de revocación está activada, los usuarios avanzados pueden especificar la siguiente configuración adicional.

  URL de OSCP

  De forma predeterminada, vCenter Single Sign-On verifica la ubicación del respondedor OCSP que se define en el certificado que se está validando. Si la extensión de acceso a la información de entidad no está presente en el certificado o si desea anularla, puede especificar explícitamente una ubicación.

  Usar CRL del certificado

De forma predeterminada, vCenter Single Sign-On verifica la ubicación de CRL que se define en el certificado que se está validando. Desactive esta opción si el certificado no incluye la extensión del punto de distribución de CRL o si desea anular la que se define de forma predeterminada.

Ubicación de CRL

Utilice esta propiedad si desactiva **Usar CRL del certificado** y desea especificar una ubicación (archivo o URL HTTP) en donde se encuentra la CRL.

Puede agregar una directiva de certificados para limitar aún más los certificados que acepta vCenter Single Sign-On.

Requisitos previos

- Compruebe que en su entorno se haya configurado una infraestructura de clave pública (Public Key Infrastructure, PKI) empresarial, y que los certificados cumplan con los siguientes requerimientos:
  - Un nombre principal de usuario (User Principal Name, UPN) debe corresponder a una cuenta de Active Directory en la extensión del nombre alternativo del firmante (Subject Alternative Name, SAN).
  - El certificado debe especificar la autenticación del cliente en los campos Directiva de aplicación o Uso mejorado de clave; de lo contrario, el explorador no mostrará el certificado.
- Compruebe que el certificado de vCenter Server sea de confianza para la instancia de Workstation del usuario final. De lo contrario, el explorador no intentará la autenticación.
- Agregue un origen de identidad de Active Directory a vCenter Single Sign-On.
- Asigne la función de Administrador de vCenter Server a uno o más usuarios en el origen de identidad de Active Directory. Posteriormente, esos usuarios pueden realizar tareas de autenticación debido a que poseen privilegios de administrador de vCenter Server.

Procedimiento

1. Inicie sesión con vSphere Client en vCenter Server.
2. Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.
3. Desplácese hasta la interfaz de usuario de configuración.
   a. En el menú **Inicio**, seleccione **Administración**.
   b. En **Single Sign On**, haga clic en **Configuración**.
4. En la pestaña **Proveedor de identidad**, haga clic en **Autenticación de tarjeta inteligente**.
5. Haga clic en **Revocación de certificado** y haga clic en **Editar** para activar o desactivar la comprobación de revocación.

6 Si en su entorno hay directivas de certificados vigentes, puede agregar una directiva en el panel **Directivas de certificado**.

Configurar la autenticación de RSA SecurID

Se puede configurar el entorno de manera que se solicite a los usuarios iniciar sesión con un token RSA SecurID. La configuración de SecurID solo es compatible desde la línea de comandos.

Para obtener más información, consulte las dos publicaciones del blog de vSphere sobre la configuración de RSA SecurID.

Nota RSA Authentication Manager requiere que el identificador de usuario sea único, y que utilice entre 1 y 255 caracteres ASCII. Los caracteres Y comercial (&), porcentaje (%), mayor que (>), menor que (<) y apóstrofo (`) no están permitidos.

Requisitos previos

- Compruebe que RSA Authentication Manager se haya configurado correctamente en el entorno y que los usuarios disponen de tokens RSA.Compruebe que RSA Authentication Manager se haya configurado correctamente en el entorno y que los usuarios dispongan de tokens RSA. Se requiere RSA Authentication Manager versión 8.0 o posterior.
- Compruebe que el origen de identidad que utiliza RSA Manager se haya agregado a vCenter Single Sign-On. Consulte Agregar o editar un origen de identidad vCenter Single Sign-On.
- Compruebe que el sistema RSA Authentication Manager pueda resolver el nombre de host de vCenter Server y que el sistema vCenter Server pueda resolver el nombre de host de RSA Authentication Manager.
- Exporte el archivo `sdconf.rec` desde la instancia de RSA Manager seleccionando **Acceso > Agentes de autenticación > Generar archivo de configuración**. Para encontrar el archivo `sdconf.rec`, descomprima el archivo `AM_Config.zip` resultante.
- Copie el archivo `sdconf.rec` en el nodo vCenter Server.

Procedimiento

1 Pase al directorio donde se ubica el script de `sso-config`.

```
/opt/vmware/bin
```

2 Para activar la autenticación RSA SecurID y ejecute el siguiente comando.

```
sso-config.sh -t tenantName -set_authn_policy -securIDAuthn true
```

tenantName es el nombre del dominio vCenter Single Sign-On, vsphere.local de forma predeterminada.

3 (opcional) Para desactivar otros métodos de autenticación, ejecute el siguiente comando.

```
sso-config.sh -set_authn_policy -pwdAuthn false -winAuthn false -certAuthn false -t
vsphere.local
```

4 Para configurar el entorno de forma que el tenant del sitio actual utilice el sitio de RSA, ejecute el siguiente comando.

```
sso-config.sh -set_rsa_site [-t tenantName] [-siteID Location] [-agentName Name] [-
sdConfFile Path]
```

Por ejemplo:

```
sso-config.sh -set_rsa_site -agentName SSO_RSA_AUTHSDK_AGENT -sdConfFile /tmp/sdconf.rec
```

Puede especificar las siguientes opciones.

Opción	Descripción
siteID	Identificador opcional del sitio de Platform Services Controller. Platform Services Controller admite una instancia de RSA Authentication Manager o clúster por sitio. Si no especifica esta opción de manera explícita, la configuración de RSA se destina al sitio de Platform Services Controller actual. Solo utilice esta opción si desea agregar un sitio diferente.
agentName	Definido en RSA Authentication Manager.
sdConfFile	Copia del archivo `sdconfig.rec` que se descargó de RSA Manager, el cual incluye la información de configuración de RSA Manager (por ejemplo, la dirección IP).

5 (opcional) Para cambiar la configuración del tenant para que utilice valores distintos a los predeterminados, ejecute el siguiente comando.

```
sso-config.sh -set_rsa_config [-t tenantName] [-logLevel Level] [-logFileSize Size]
[-maxLogFileCount Count] [-connTimeOut Seconds] [-readTimeOut Seconds] [-encAlgList
Alg1,Alg2,...]
```

El valor predeterminado suele ser adecuado, por ejemplo:

```
sso-config.sh -set_rsa_config -t vsphere.local -logLevel DEBUG
```

6 (opcional) Si el origen de identidad no utiliza el nombre principal de usuario como identificador del usuario, configure el atributo userID del origen de identidad. (Compatible solo con orígenes de identidad de Active Directory en LDAP).

El atributo userID determina qué atributo LDAP se utiliza como userID en RSA.

```
sso-config.sh -set_rsa_userid_attr_map [-t tenantName] [-idsName Name] [-ldapAttr
AttrName] [-siteID Location]
```

Por ejemplo:

```
sso-config.sh -set_rsa_userid_attr_map -t vsphere.local -idsName ssolabs.com -ldapAttr
userPrincipalName
```

7 Para mostrar la configuración actual, ejecute el siguiente comando.

```
sso-config.sh -t tenantName -get_rsa_config
```

Resultados

Si la autenticación por nombre de usuario y contraseña no está activada, pero la autenticación de RSA sí lo está, los usuarios deben iniciar sesión con el nombre de usuario y el token RSA. Ya no es posible iniciar sesión con el nombre de usuario y la contraseña.

Nota Use el formato de nombre de usuario ***userID@domainName*** o ***userID@domain_upn_suffix***.

Administrar el mensaje de inicio de sesión en la página de inicio de sesión de vSphere Client

Puede crear un mensaje que aparezca en la página de inicio de sesión de vSphere Client.

Puede establecer un mensaje, un descargo de responsabilidad o términos y condiciones. Además, puede configurar el mensaje para solicitar la confirmación del mensaje antes de iniciar sesión.

Administrar el mensaje de inicio de sesión en la página de inicio de sesión de vSphere Client

Puede agregar un mensaje de inicio de sesión a la página de inicio de sesión de vSphere Client. También puede configurar un mensaje de inicio de sesión personalizado y proporcionar una casilla de verificación para el consentimiento del usuario.

Procedimiento

1 Inicie sesión con vSphere Client en vCenter Server.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

a En el menú **Inicio**, seleccione **Administración**.

b En **Single Sign On**, haga clic en **Configuración**.

4 Haga clic en la pestaña **Mensaje de inicio de sesión**.

5 Haga clic en **Editar** y configure el mensaje de inicio de sesión.

Opción	Descripción
Mostrar mensaje de inicio de sesión	Alterne **Mostrar el mensaje de inicio de sesión** para habilitar el mensaje de inicio de sesión. No se pueden realizar cambios en el mensaje de inicio de sesión a menos que alterne este conmutador.
Mensaje de inicio de sesión	Título del mensaje. De forma predeterminada, cuando se alterna la **casilla de consentimiento**, el texto del mensaje de inicio de sesión es `I agree to Terms and Conditions`. Debe reemplazar `Terms and Conditions` con su propio texto. Si la **Casilla de verificación de consentimiento** está desactivada, a continuación aparece `Login message` donde deberá escribir el mensaje.
Casilla de consentimiento	Alterne la **casilla de consentimiento** para requerir que el usuario haga clic en una casilla antes de iniciar sesión. También se puede mostrar un mensaje sin ninguna casilla.
Detalles del mensaje de inicio de sesión	Mensaje que ve el usuario cuando hace clic en el mensaje de inicio de sesión, por ejemplo, el texto de los términos y las condiciones. Debe introducir algunos detalles en este cuadro de texto.

6 Haga clic en **Guardar**.

Prácticas recomendadas de seguridad de vCenter Single Sign-On

Siga las prácticas recomendadas de seguridad de vCenter Single Sign-On para proteger el entorno de vSphere.

La infraestructura de autenticación de vSphere mejora la seguridad del entorno de vSphere. Para garantizar que la infraestructura no se vea comprometida, siga las prácticas recomendadas de vCenter Single Sign-On.

Compruebe la caducidad de las contraseñas

La directiva predeterminada de contraseñas de vCenter Single Sign-On establece una duración de 90 días para las contraseñas. Después de 90 días, la contraseña caduca y ya no puede iniciar sesión. Compruebe la fecha de caducidad y actualice las contraseñas oportunamente.

Configurar el protocolo de tiempo de redes

Use el protocolo de hora de red (Network Time Protocol, NTP) para garantizar que todos los sistemas tengan el mismo origen de hora relativo (incluida la correspondiente compensación por localización), y que este pueda ser correlativo con una hora estándar acordada (como la hora universal— UTC). La sincronización de los sistemas es fundamental para la validez de los certificados de vCenter Single Sign-On y de otros certificados de vSphere.

NTP también facilita el rastreo de intrusos en los archivos de registro. Una configuración incorrecta de la hora puede dificultar la inspección y la correlación de los archivos de registro a fin de detectar ataques; también puede hacer imprecisas las auditorías.

Consulte la documentación de *Seguridad de vSphere* para obtener instrucciones sobre cómo configurar la sincronización de hora mediante NTP.

Solucionar problemas de autenticación de vCenter Server

5

Los siguientes temas ofrecen un punto de partida para la solución de problemas de autenticación de vCenter Server. Para más información, busque en este centro de documentación y en la base de conocimientos de VMware.

Lea los siguientes temas a continuación:

Determinar la causa de un error de Lookup Service

La instalación de vCenter Single Sign-On muestra un error relacionado con vCenter Server o con vSphere Client.

Problema

Los programas de instalación de vCenter Server y Web Client muestran el error `Could not contact Lookup Service. Please check VM_ssoreg.log....`

Causa

Este problema tiene varias causas, como relojes no sincronizados en los equipos host, bloqueos de firewall y servicios que deben iniciarse.

Solución

1 Compruebe que los relojes de los equipos host que ejecutan vCenter Single Sign-On, vCenter Server y Web Client estén sincronizados.

2 Vea el archivo de registro específico que se encuentra en el mensaje de error.

   En el mensaje, la carpeta temporal del sistema hace referencia a `%TEMP%`.

3 En el archivo de registro, busque los siguientes mensajes.

El archivo de registro contiene una salida de todos los intentos de instalación. Busque el último mensaje que muestra Initializing registration provider...

Mensaje	Causa y solución
java.net.ConnectException: Connection timed out: connect	La dirección IP es incorrecta, hay un firewall bloqueando el acceso a vCenter Single Sign-On o vCenter Single Sign-On está sobrecargado. Asegúrese de que un firewall no esté bloqueando el puerto de vCenter Single Sign-On (de manera predeterminada es el 7444). Compruebe también que el equipo donde está instalado vCenter Single Sign-On tenga suficiente capacidad libre de CPU, RAM y E/S.
java.net.ConnectException: Connection refused: connect	La dirección IP o el FQDN son incorrectos y el servicio vCenter Single Sign-On no se inició o se inició en el último minuto. Compruebe que vCenter Single Sign-On funciona. Para ello, consulte el estado del daemon vmware-sso de vCenter Single Sign-On. Reinicie el servicio. Si el reinicio no soluciona el problema, consulte la sección Recuperación de la guía *Solucionar problemas de vSphere*.
Unexpected status code: 404. SSO Server failed during initialization	Reinicie vCenter Single Sign-On. Si el reinicio no soluciona el problema, consulte la sección Recuperación de la guía *Solucionar problemas de vSphere*.
El error que se muestra en la interfaz de usuario comienza con Could not connect to vCenter Single Sign-On	También se observa el código de retorno SslHandshakeFailed. Este error indica que la dirección IP o el FQDN proporcionados que se resuelven en el host de vCenter Single Sign-On no era la dirección que se utilizó cuando se instaló vCenter Single Sign-On. En VM_ssoreg.log, busque la línea que contiene el siguiente mensaje. host name in certificate did not match: <install-configured FQDN or IP> != <A> or <B> or <C> donde A era el FQDN que se introdujo durante la instalación de vCenter Single Sign-On, y B y C eran las alternativas permitidas generadas por el sistema. Corrija la configuración para utilizar el FQDN a la derecha del signo != del archivo de registro. En la mayoría de los casos, utilice el FQDN que especificó durante la instalación de vCenter Single Sign-On. Si ninguna de las alternativas es posible en la configuración de la red, recupere la configuración de SSL de vCenter Single Sign-On.

No se puede iniciar sesión con la autenticación del dominio de Active Directory

Se inicia sesión en un componente de vCenter Server desde vSphere Client. Se utiliza el nombre de usuario y la contraseña de Active Directory. Se produce un error en la autenticación.

Problema

Se agrega el origen de identidad de Active Directory a vCenter Single Sign-On, pero los usuarios no pueden iniciar sesión en vCenter Server.

Causa

Los usuarios utilizan su nombre de usuario y contraseña para iniciar sesión en el dominio predeterminado. Para los demás dominios, los usuarios deben incluir el nombre de dominio (usuario@dominio o DOMINIO\usuario).

Solución

En todas las implementaciones de vCenter Single Sign-On, se puede cambiar el origen de identidad predeterminado. Después de ese cambio, los usuarios pueden iniciar sesión en el origen de identidad predeterminado únicamente con el nombre de usuario y la contraseña.

Para configurar un origen de identidad para Autenticación integrada de Windows con un dominio secundario dentro del bosque de Active Directory, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2070433. De forma predeterminada, la autenticación integrada de Windows utiliza el dominio raíz del bosque de Active Directory.

Si cambiar el origen de identidad predeterminado no soluciona el problema, siga estos pasos adicionales de solución de problemas.

1 Sincronice los relojes entre vCenter Server y las controladoras de dominio de Active Directory.

2 Compruebe que cada controlador de dominio tenga un registro de puntero (pointer record, PTR) en el servicio DNS del dominio de Active Directory.

   Compruebe que la información del registro PTR para el controlador de dominio coincida con el nombre DNS del controlador. Al utilizar vCenter Server, ejecute los siguientes comandos para realizar la tarea:

   a Para enumerar los controladores de dominio, ejecute el siguiente comando:

      ```
      # dig SRV _ldap._tcp.my-ad.com
      ```

      Las direcciones relevantes aparecen en la sección de respuestas, como en el ejemplo siguiente:

      ```
      ;; ANSWER SECTION:
      _ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
      ...
      ```

   b Para cada controladora de dominio, compruebe la resolución de nombres en las direcciones IP (conocida como forward) y la resolución inversa mediante el comando siguiente:

      ```
      # dig my-controller.my-ad.com
      ```

Las direcciones relevantes aparecen en la sección de respuestas, como en el ejemplo siguiente:

```
;; ANSWER SECTION:
my-controller.my-ad.com (...) IN A controller IP address
...
```

```
# dig -x <controller IP address>
```

Las direcciones relevantes aparecen en la sección de respuestas, como en el ejemplo siguiente:

```
;; ANSWER SECTION:
IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
...
```

3 Si esto no soluciona el problema, quite vCenter Server del dominio de Active Directory y vuelva a asociar el dominio. Consulte la documentación de *Configuración de vCenter Server*.

4 Cierre todas las sesiones del explorador que estén conectadas a vCenter Server y reinicie los servicios.

```
/bin/service-control --restart --all
```

Se produce un error en el inicio de sesión en vCenter Server porque la cuenta de usuario está bloqueada

Al iniciar sesión en vCenter Server desde la página de inicio de sesión de vSphere Client, un error indica que la cuenta está bloqueada.

Problema

Después de varios intentos con errores, no puede iniciar sesión en vSphere Client mediante vCenter Single Sign-On. Aparece un mensaje que indica que la cuenta está bloqueada.

Causa

Se supera la cantidad máxima de intentos de inicio de sesión con errores.

Solución

- Si intentó iniciar sesión como usuario desde el dominio del sistema (vsphere.local de manera predeterminada), solicítele al administrador de vCenter Single Sign-On que desbloquee la cuenta. Si el bloqueo está configurado para caducar en la directiva de bloqueo, puede esperar hasta que la cuenta se desbloquee. Los administradores de vCenter Single Sign-On pueden usar comandos de CLI para desbloquear la cuenta.
- Si inicia sesión como usuario desde el dominio de Active Directory o de LDAP, solicítele al administrador de Active Directory o LDAP que desbloquee la cuenta.

La replicación de VMware Directory Service puede tardar mucho

Si el entorno incluye varias instancias de vCenter Server conectadas a través de Enhanced Linked Mode, y si una de las instancias de vCenter Server deja de estar disponible, el entorno continúa funcionando. Cuando vCenter Server vuelve a estar disponible, se suelen replicar los datos del usuario y otra información en un plazo de 30 segundos con socios conectados a través de Enhanced Linked Mode. Sin embargo, ante algunas circunstancias, la replicación puede tardar mucho.

Problema

En ciertas situaciones, por ejemplo, cuando el entorno incluye varias instancias de vCenter Server en diferentes ubicaciones, y se realizan cambios significativos mientras una instancia de vCenter Server no está disponible, no se ve de inmediato la replicación en todas las instancias de VMware Directory Service. Por ejemplo, el usuario nuevo que se agregó a la instancia disponible de vCenter Server no se puede ver en la otra instancia hasta que la replicación está completa. La replicación puede tardar mucho tiempo, en función de la topología de Enhanced Linked Mode.

Causa

En condiciones de funcionamiento normal, los cambios que se realizan en la instancia de VMware Directory Service (vmdir) en una instancia de vCenter Server (nodo) aparecen en su partner de replicación directo en un plazo de 30 segundos. Según la topología de la replicación, es posible que los cambios realizados en un nodo deban propagarse por nodos intermedios antes de llegar a cada instancia de vmdir en cada nodo. La información que se replica incluye información del usuario, de certificados, de licencias para las máquinas virtuales creadas, clonadas o migradas con VMware vMotion, entre otras.

Cuando se rompe el vínculo de replicación, por ejemplo, debido a una interrupción de la red o porque un nodo dejó de estar disponible, los cambios en la federación no convergen. Una vez que se restaura el nodo no disponible, cada nodo intenta actualizarse con todos los cambios. Finalmente, todas las instancias de vmdir convergen en un estado coherente, pero puede llevar un tiempo alcanzar ese estado si se produjeron muchos cambios mientras un nodo no estaba disponible.

Solución

El entorno funciona con normalidad mientras se lleva a cabo la replicación. No intente resolver el problema a menos que persista durante más de una hora.

Exportar un paquete de soporte de vCenter Server

Puede exportar un paquete de soporte que contenga los archivos de registro de los servicios de vCenter Server de vSphere Client o mediante una API. Después de la exportación, puede explorar los registros localmente o enviar el paquete al soporte técnico de VMware.

Para obtener más información sobre la API, consulte *Guía de programación de administración de vCenter Server*.

Requisitos previos

Compruebe que vCenter Server esté implementado y ejecutándose correctamente.

Procedimiento

1 Desde un explorador web, conéctese a la interfaz de administración de configuración de vCenter Server en https://*vcenter_server_ip*:5480.

2 Inicie sesión como usuario raíz para la instancia de vCenter Server.

3 En el menú **Acciones**, seleccione **Crear paquete de soporte**.

4 El paquete de soporte se guarda en la máquina local, a menos que la configuración del explorador evite una descarga inmediata.

Referencia a registros de servicios de autenticación de vCenter Server

Los servicios de autenticación de vCenter Server usan Syslog para el registro. Puede examinar los archivos de registro para determinar cuáles son las causas de los errores.

Tabla 5-1. Registros de servicios de autenticación de vCenter Server

Servicio	Descripción
VMware Directory Service	De manera predeterminada, el registro de vmdir va a `/var/log/messages` o `/var/log/vmware/vmdird/`. Para los problemas en el tiempo de implementación, `/var/log/vmware/vmdir/vmafdvmdirclient.log` también puede contener datos útiles sobre solución de problemas.
VMware Single Sign-On	El registro de vCenter Single Sign-On va a `/var/log/vmware/sso/`.
VMware Certificate Authority (VMCA)	El registro del servicio VMCA se encuentra en `/var/log/vmware/vmcad/vmcad-syslog.log`.
Almacén de certificados de endpoints de VMware (VECS)	El registro del servicio VECS se encuentra en `/var/log/vmware/vmafdd/vmafdd-syslog.log`.
VMware Lookup Service	El registro del servicio de búsqueda se encuentra en `/var/log/vmware/sso/lookupServer.log`.